Options pour réduire les intrusions de faux positifs

Table des matières

Introduction

Options de réduction des alertes de faux positifs

- 1. Signaler au support technique de Cisco
- 2. Règle d'approbation ou d'autorisation
- 3. Désactiver les règles inutiles
- 4. Seuil
- 5. Répression
- 6. Règles de Fast Path
- 7. Règles d'acceptation
- 8. Variable SNORT_BPF

Introduction

Un système de prévention des intrusions peut générer des alertes excessives sur une certaine règle Snort. Les alertes peuvent être de vrais positifs ou de faux positifs. Si vous recevez de nombreuses alertes de faux positifs, plusieurs options sont disponibles pour vous permettre de les réduire. Cet article résume les avantages et les inconvénients de chaque option.

Options de réduction des alertes de faux positifs

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

1. Signaler au support technique de Cisco

Si vous trouvez une règle Snort qui déclenche des alertes sur le trafic inoffensif, veuillez la signaler au support technique de Cisco. Une fois le problème signalé, un ingénieur du support technique le signale à l'équipe VRT (Vulnerability Research Team). La VRT recherche les améliorations possibles de la règle. Les règles améliorées sont généralement disponibles pour le rapporteur dès qu'elles sont disponibles et sont également ajoutées à la prochaine mise à jour officielle des règles.

2. Règle d'approbation ou d'autorisation

La meilleure option pour permettre au trafic approuvé de passer par une appliance Sourcefire sans inspection est d'activer l'action Trust ou Allow sans une stratégie d'intrusion associée. Pour

configurer une règle d'approbation ou d'autorisation, accédez à Politiques > Contrôle d'accès > Ajouter une règle.

> Remarque : Le trafic correspondant aux règles d'approbation ou d'autorisation qui ne sont pas configurées pour correspondre aux utilisateurs, aux applications ou aux URL aura un impact minimal sur les performances globales d'une appliance Sourcefire, car ces règles peuvent être traitées dans le matériel FirePOWER.

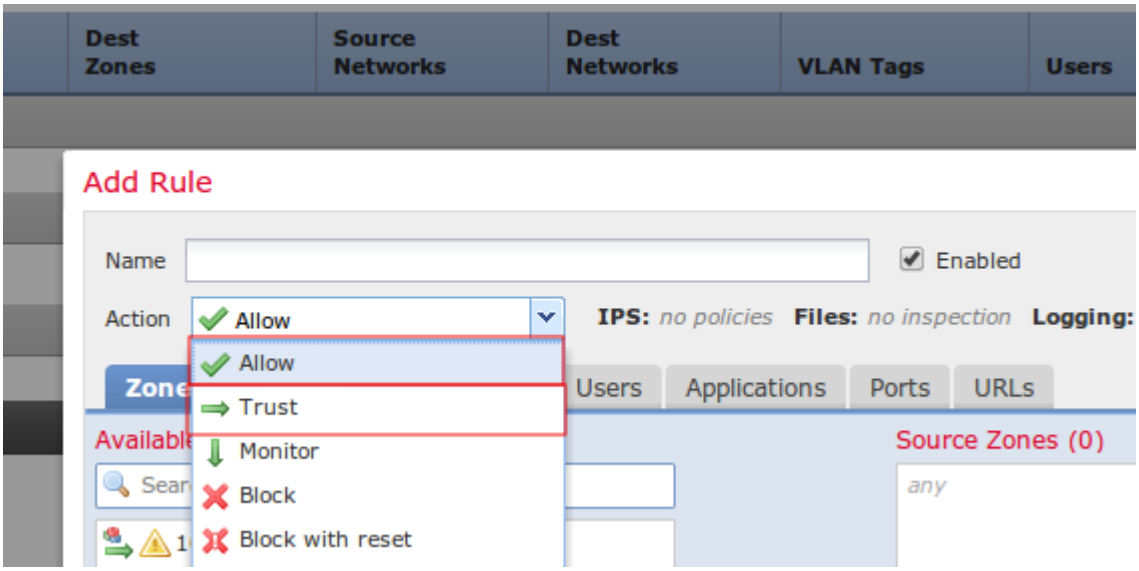


Figure : Configuration d'une règle de confiance

3. Désactiver les règles inutiles

Vous pouvez désactiver les règles Snort qui ciblent les vulnérabilités anciennes et corrigées. Il améliore les performances et réduit le nombre de faux positifs. Les recommandations FireSIGHT peuvent vous aider dans cette tâche. En outre, les règles qui génèrent fréquemment des alertes de faible priorité ou des alertes qui ne sont pas exploitables peuvent être de bons candidats pour la suppression d'une stratégie d'intrusion.

4. Seuil

Vous pouvez utiliser Threshold pour réduire le nombre d'événements d'intrusion. Il s'agit d'une bonne option à configurer lorsqu'une règle est censée déclencher régulièrement un nombre limité d'événements sur le trafic normal, mais elle peut être une indication d'un problème si plus d'un certain nombre de paquets correspondent à la règle. Vous pouvez utiliser cette option pour réduire le nombre d'événements déclenchés par des règles bruyantes.

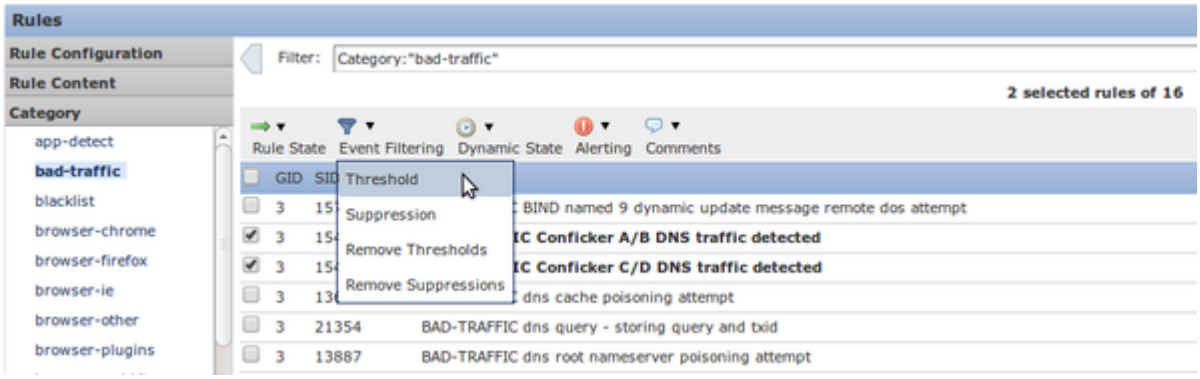


Figure : Configuration du seuil

5. Répression

Vous pouvez utiliser Suppression pour éliminer complètement la notification d'événements. Il est configuré de la même manière que l'option Seuil.

Mise en garde : La suppression peut entraîner des problèmes de performances, car même si aucun événement n'est généré, Snort doit toujours traiter le trafic.

Remarque : La suppression n'empêche pas les règles d'abandon d'abandonner le trafic. Le trafic peut donc être abandonné en silence lorsqu'il correspond à la règle d'abandon.

---

6. Règles de Fast Path

Tout comme les règles Trust et Allow d'une politique de contrôle d'accès, les règles FastPath peuvent également contourner l'inspection. L'assistance technique de Cisco ne recommande généralement pas l'utilisation des règles Fast-Path car elles sont configurées dans la fenêtre Advanced de la page Device et peuvent être facilement ignorées alors que les règles de contrôle d'accès sont presque toujours suffisantes.

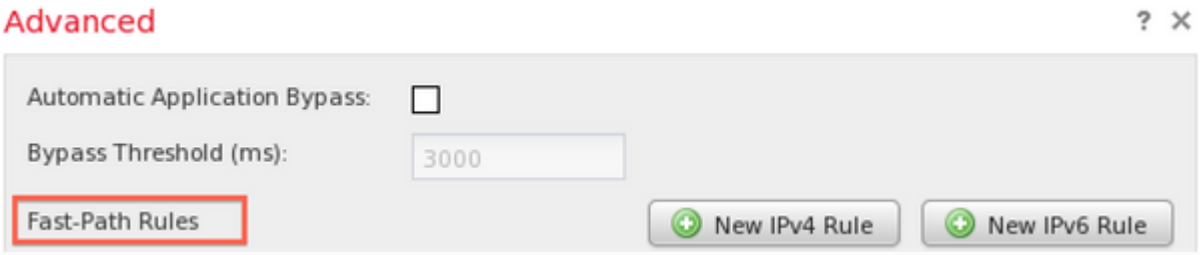


Figure : Fast-Path Rules dans la fenêtre Advanced.

Le seul avantage des règles de chemin rapide est qu'elles peuvent gérer un plus grand volume de trafic maximum. Les règles de chemin rapide traitent le trafic au niveau matériel (connu sous le nom de NMSB) et peuvent théoriquement gérer jusqu'à 200 Gbit/s de trafic. En revanche, les règles avec les actions Trust et Allow sont promues au Network Flow Engine (NFE) et peuvent gérer un maximum de 40 Gbit/s de trafic.

Remarque : Les règles Fast Path ne sont disponibles que sur les périphériques de la gamme 8000 et le 3D9900.

7. Règles d'acceptation

Afin d'empêcher une règle spécifique de se déclencher sur le trafic d'un certain hôte (tandis que d'autres trafics de cet hôte doivent être inspectés), utilisez une règle de passe de type Snort. En fait, c'est la seule façon de le faire. Bien que les règles d’acceptation soient efficaces, elles peuvent être très difficiles à gérer car elles sont écrites manuellement. En outre, si les règles d'origine des règles d'exécution sont modifiées par une mise à jour de règle, toutes les règles d'exécution associées doivent être mises à jour manuellement. Dans le cas contraire, ils risquent de devenir inefficaces.

8. Variable SNORT_BPF

La variable Snort_BPF dans une politique d'intrusion permet à un certain trafic de contourner l'inspection. Bien que cette variable ait été l'un des premiers choix sur les versions logicielles héritées, l'assistance technique de Cisco recommande d'utiliser une règle de contrôle d'accès pour contourner l'inspection, car elle est plus granulaire, plus visible et beaucoup plus facile à configurer.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.