Optionen zur Verringerung von Fehlalarmen

Inhalt

Einführung

Ein Intrusion Prevention System kann bei einer bestimmten Snort-Regel übermäßige Warnungen auslösen. Die Warnmeldungen können entweder echt positiv oder falsch positiv sein. Wenn Sie viele Fehlalarme erhalten, stehen Ihnen mehrere Möglichkeiten zur Verfügung, diese zu reduzieren. Dieser Artikel enthält eine Zusammenfassung der Vor- und Nachteile jeder Option.

Optionen zur Verringerung von Fehlalarmen

> **Hinweis**: Diese Optionen sind in der Regel nicht die beste Wahl, sondern können unter bestimmten Umständen die einzige Lösung sein.

1. Bericht an den technischen Support von Cisco

Wenn Sie eine Snort-Regel finden, die Warnungen für gutartigen Datenverkehr auslöst, teilen Sie diese bitte dem technischen Support von Cisco mit. Nach der Meldung eskaliert ein Customer Support Engineer das Problem an das Vulnerability Research Team (VRT). VRT recherchiert mögliche Verbesserungen an der Regel. Verbesserte Regeln stehen dem Reporter in der Regel zur Verfügung, sobald sie verfügbar sind, und werden auch zum nächsten offiziellen Regelupdate hinzugefügt.

2. Trust oder Allow Rule

Die beste Option, um zu erlauben, dass vertrauenswürdiger Datenverkehr eine Sourcefire-Appliance ohne Prüfung durchläuft, besteht in der Aktivierung von **Trust**- oder **Allow-**Aktionen ohne zugeordnete Zugriffsrichtlinien. Um eine Vertrauenswürdigkeit- oder Zulassen-Regel zu konfigurieren, navigieren Sie zu **Richtlinien > Zugriffskontrolle > Regel hinzufügen**.

> **Hinweis**: Datenverkehr, der mit Trust- oder Allow-Regeln übereinstimmt, die nicht so konfiguriert sind, dass Benutzer, Anwendungen oder URLs übereinstimmen, hat nur

minimale Auswirkungen auf die Gesamtleistung einer Sourcefire-Appliance, da diese Regeln in der FirePOWER-Hardware verarbeitet werden können.

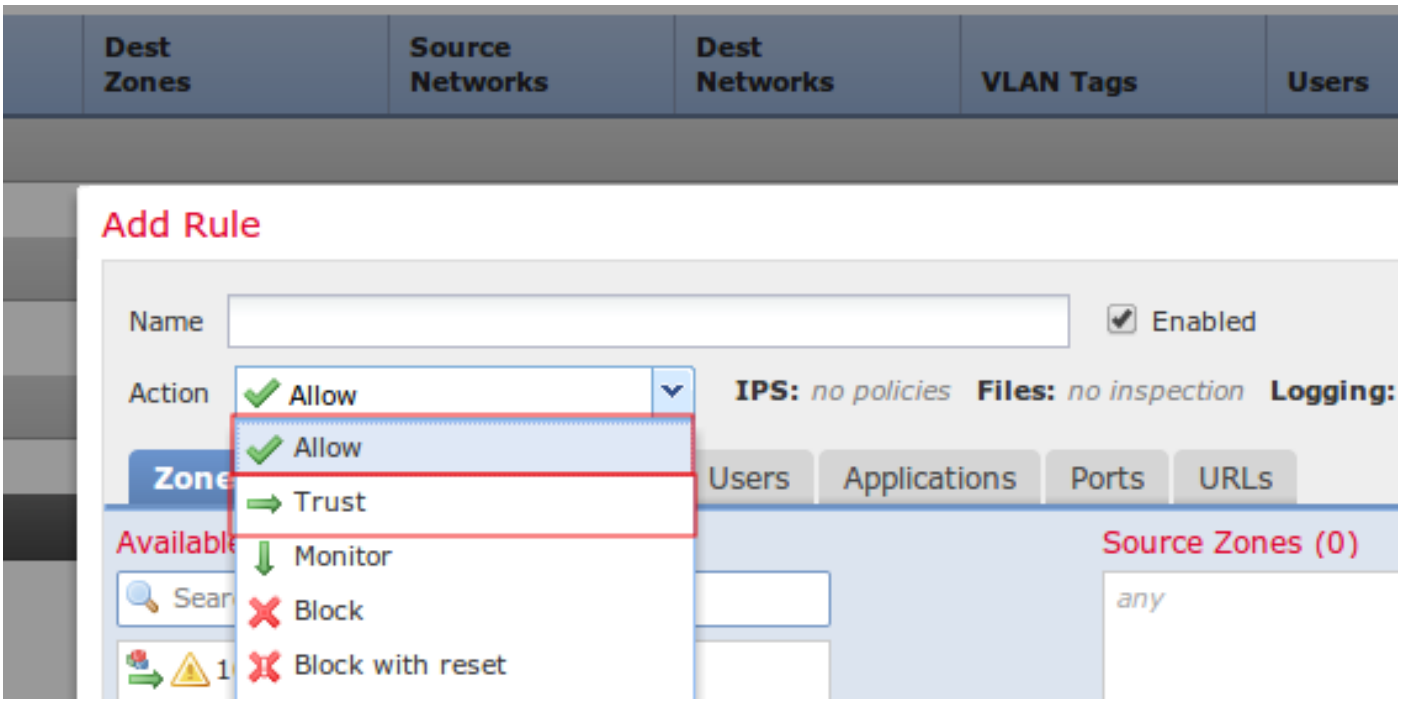

Abbildung: Konfiguration einer Vertrauensregel

3. Unnötige Regeln deaktivieren

Sie können Snort-Regeln deaktivieren, die auf alte und gepatchte Schwachstellen abzielen. Es verbessert die Leistung und reduziert Fehlalarme. Die Verwendung von FireSIGHT-Empfehlungen kann bei dieser Aufgabe hilfreich sein. Regeln, die häufig Warnungen mit niedriger Priorität oder Warnungen auslösen, die nicht umsetzbar sind, können sich auch als gute Kandidaten für die Entfernung aus einer Richtlinie für Sicherheitsrisiken erweisen.

4. Grenzwert

Sie können **Threshold** verwenden, um die Anzahl von Angriffsversuchen zu reduzieren. Dies ist eine gute Option, wenn bei einer Regel erwartet wird, dass sie regelmäßig eine begrenzte Anzahl von Ereignissen im normalen Datenverkehr auslöst. Dies kann jedoch ein Hinweis auf ein Problem sein, wenn mehr als eine bestimmte Anzahl von Paketen mit der Regel übereinstimmen. Mit dieser Option können Sie die Anzahl der Ereignisse reduzieren, die durch laute Regeln ausgelöst werden.

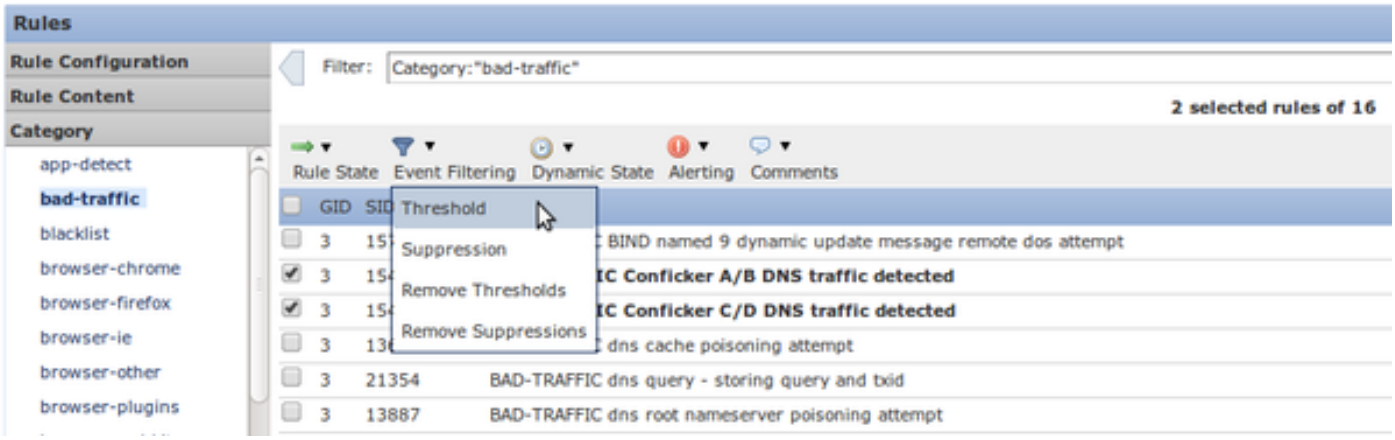

Abbildung: Konfiguration des Schwellenwerts

5. Unterdrückung

Sie können **Suppression** verwenden, um die Ereignisbenachrichtigung vollständig zu löschen. Die Konfiguration ähnelt der Option **Schwellenwert**.

> **Vorsicht**: Unterdrückung kann Leistungsprobleme verursachen, da Snort den Datenverkehr noch verarbeiten muss, während keine Ereignisse generiert werden.

> **Hinweis**: Die Unterdrückung verhindert jedoch nicht, dass Regeln den Datenverkehr verwerfen, sodass der Datenverkehr bei Übereinstimmung mit einer Regel zum Verwerfen leise fallen gelassen wird.

6. Fast-Path-Regeln

Ähnlich wie bei den Regeln Vertrauenswürdigkeit und Zulassen einer Zugriffskontrollrichtlinie können Fast-Path-Regeln auch Überprüfungen umgehen. Der technische Support von Cisco empfiehlt generell die Verwendung von Fast-Path-Regeln nicht, da diese im **erweiterten** Fenster der **Device-**Seite konfiguriert werden und leicht übersehen werden können, während Zugriffskontrollregeln fast immer ausreichend sind.

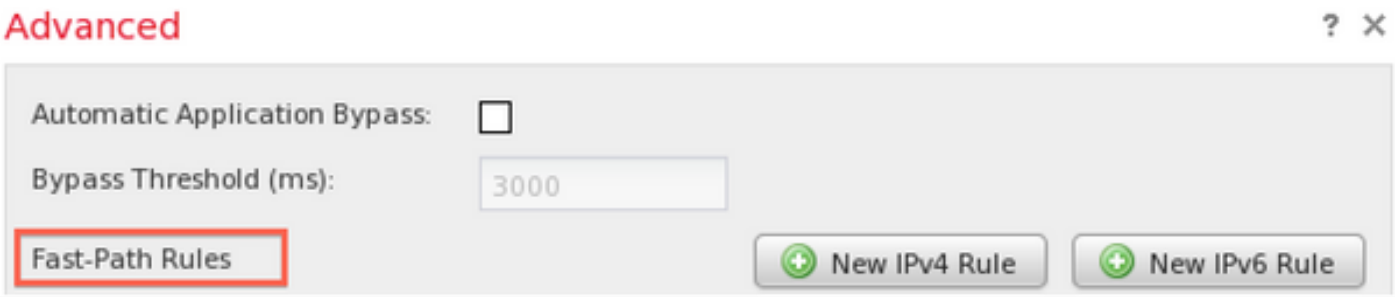

Abbildung: Die Option Fast-Path-Regeln wird im Fenster Erweitert angezeigt.

Der einzige Vorteil von Fast-Path-Regeln besteht darin, dass sie ein größeres Volumen an Datenverkehr verarbeiten können. Fast-Path-Regeln verarbeiten Datenverkehr auf Hardwareebene (NMSB) und können theoretisch bis zu 200 Gbit/s Datenverkehr verarbeiten. Im Gegensatz dazu werden Regeln mit **Trust**- und **Allow-**Aktionen auf die Network Flow Engine (NFE) hochgestuft und können bis zu 40 Gbit/s Datenverkehr verarbeiten.

Hinweis: Fast-Path-Regeln sind nur für Geräte der Serie 8000 und für 3D9900 verfügbar.

7. Regeln übergeben

Um zu verhindern, dass eine bestimmte Regel Datenverkehr von einem bestimmten Host auslöst (während anderer Datenverkehr von diesem Host überprüft werden muss), verwenden Sie eine Snort-Regel *für den* Pass. Tatsächlich ist dies der einzige Weg, dies zu erreichen. Zwar sind Pass-Regeln effektiv, sie können jedoch sehr schwer zu verwalten sein, da sie manuell verfasst werden. Wenn die ursprünglichen Regeln der Pass-Regeln durch eine Regelaktualisierung geändert werden, müssen außerdem alle zugehörigen Pass-Regeln manuell aktualisiert werden. Andernfalls können sie unwirksam werden.

8. SNORT_BPF-Variable

Die Snort_BPF-Variable in einer Intrusion Policy ermöglicht es bestimmten Datenverkehr, die Inspektion zu umgehen. Obwohl diese Variable eine der ersten Optionen für ältere Softwareversionen war, empfiehlt der technische Support von Cisco, eine Zugriffskontrollrichtlinie zu verwenden, um die Prüfung zu umgehen, da sie detaillierter, sichtbarer und wesentlich einfacher zu konfigurieren ist.