Benutzerdefinierte lokale Snort-Regeln auf einem Cisco FireSIGHT-System

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Arbeiten mit benutzerdefinierten lokalen Regeln](#)
[Lokale Regeln importieren](#)
[Lokale Regeln anzeigen](#)
[Lokale Regeln aktivieren](#)
[Gelöschte lokale Regeln anzeigen](#)
[Nummerierung der lokalen Regeln](#)

Einleitung

Eine benutzerdefinierte lokale Regel auf einem FireSIGHT-System ist eine benutzerdefinierte Snort-Standardregel, die Sie in einem ASCII-Textdateiformat von einem lokalen Computer importieren. Mit einem FireSIGHT-System können Sie lokale Regeln über die Webschnittstelle importieren. Die Schritte zum Importieren lokaler Regeln sind sehr einfach. Um jedoch eine optimale lokale Regel zu erstellen, benötigt der Benutzer fundierte Kenntnisse über Snort- und Netzwerkprotokolle.

In diesem Dokument finden Sie einige Tipps und Hinweise zum Schreiben einer benutzerdefinierten lokalen Regel. Die Anweisungen zum Erstellen lokaler Regeln finden Sie im *Snort-Benutzerhandbuch,* das unter snort.org zur Verfügung steht. Cisco empfiehlt, das Benutzerhandbuch herunterzuladen und zu lesen, bevor Sie eine benutzerdefinierte lokale Regel schreiben.

> **Anmerkung:** Die in einem Sourcefire Rule Update (SRU)-Paket enthaltenen Regeln werden von der Cisco Talos Security Intelligence and Research Group erstellt und getestet und vom Cisco Technical Assistance Center (TAC) unterstützt. Das Cisco TAC bietet keine Unterstützung beim Schreiben oder Anpassen einer benutzerdefinierten lokalen Regel. Wenden Sie sich bei Problemen mit der Funktion zum Importieren von Regeln in Ihrem FireSIGHT-System an das Cisco TAC.

> **Warnung:** Eine schlecht geschriebene benutzerdefinierte lokale Regel kann die Leistung eines FireSIGHT-Systems beeinträchtigen und so zu einer Leistungsminderung im gesamten Netzwerk führen. Wenn in Ihrem Netzwerk Leistungsprobleme auftreten und in Ihrem FireSIGHT-System einige benutzerdefinierte Snort-Regeln aktiviert sind, empfiehlt

Cisco, diese lokalen Regeln zu deaktivieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu Snort-Regeln und zum FireSIGHT-System verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Das FireSIGHT Management Center (auch bekannt als Defense Center)
- Softwareversion 5.2 oder höher

Arbeiten mit benutzerdefinierten lokalen Regeln

Lokale Regeln importieren

Bevor Sie beginnen, müssen Sie sicherstellen, dass die Regeln in der Datei keine Escapezeichen enthalten. Für den Regelimporteur müssen alle benutzerdefinierten Regeln mit ASCII- oder UTF-8-Codierung importiert werden.

Im folgenden Verfahren wird erläutert, wie Sie lokale Standardtextregeln von einem lokalen Computer importieren:

1. Rufen Sie die Seite **Regel-Editor** auf, indem Sie zu **Richtlinien > Eindringen > Regel-Editor** navigieren.

2. Klicken Sie auf **Regeln importieren**. Die Seite **Regelaktualisierungen** wird angezeigt.

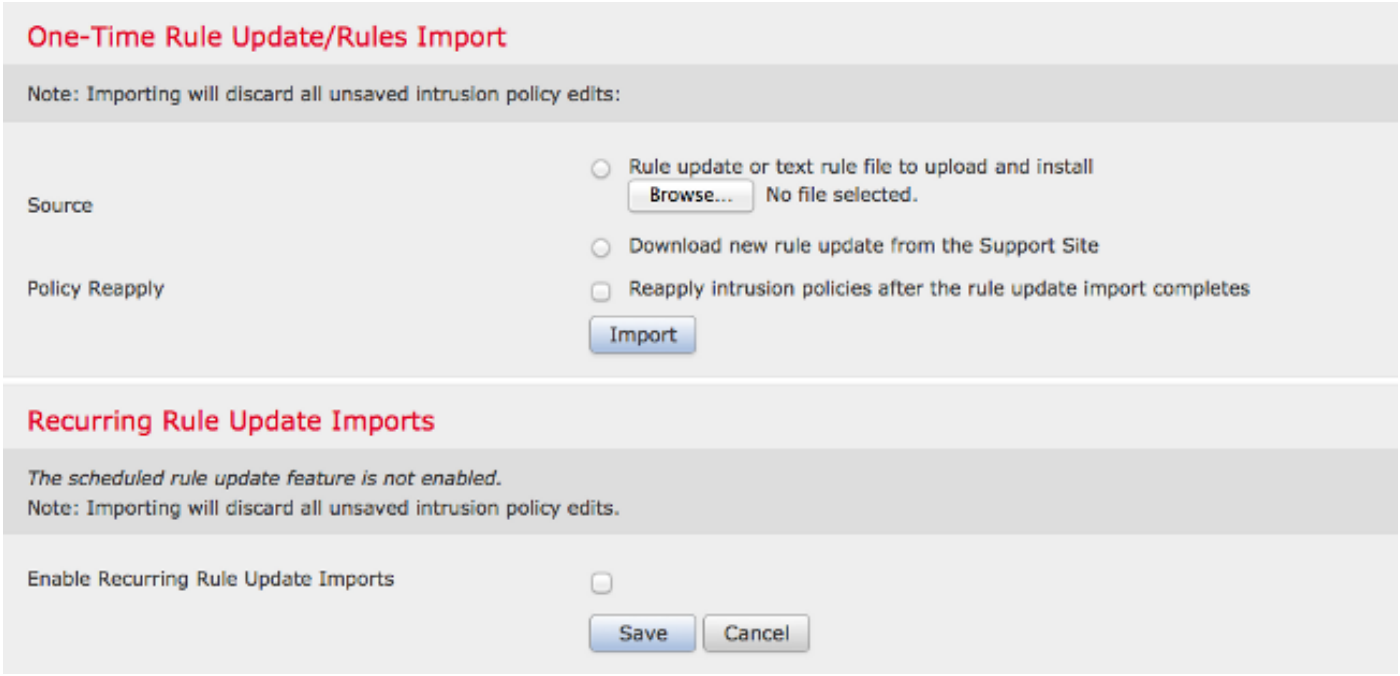


Abbildung: Screenshot der Seite Regelaktualisierungen

3. Wählen Sie **Regelaktualisierung oder Textregeldatei, die hochgeladen und installiert werden soll,** und klicken Sie auf **Durchsuchen**, um die Regeldatei auszuwählen.

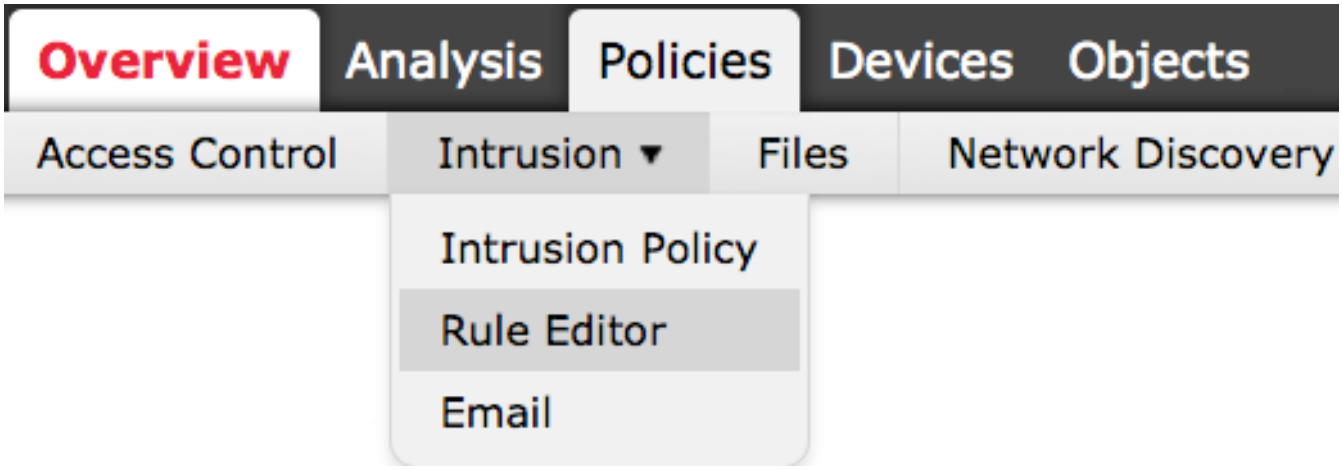
> **Anmerkung:** Alle hochgeladenen Regeln werden in der Kategorie der **lokalen Regel** gespeichert.

4. Klicken Sie auf **Importieren**. Die Regeldatei wird importiert.

> **Vorsicht:** Die FireSIGHT-Systeme verwenden den neuen Regelsatz nicht für die Inspektion. Um eine lokale Regel zu aktivieren, müssen Sie sie in der Richtlinie für Sicherheitsrisiken aktivieren und dann die Richtlinie anwenden.

Lokale Regeln anzeigen

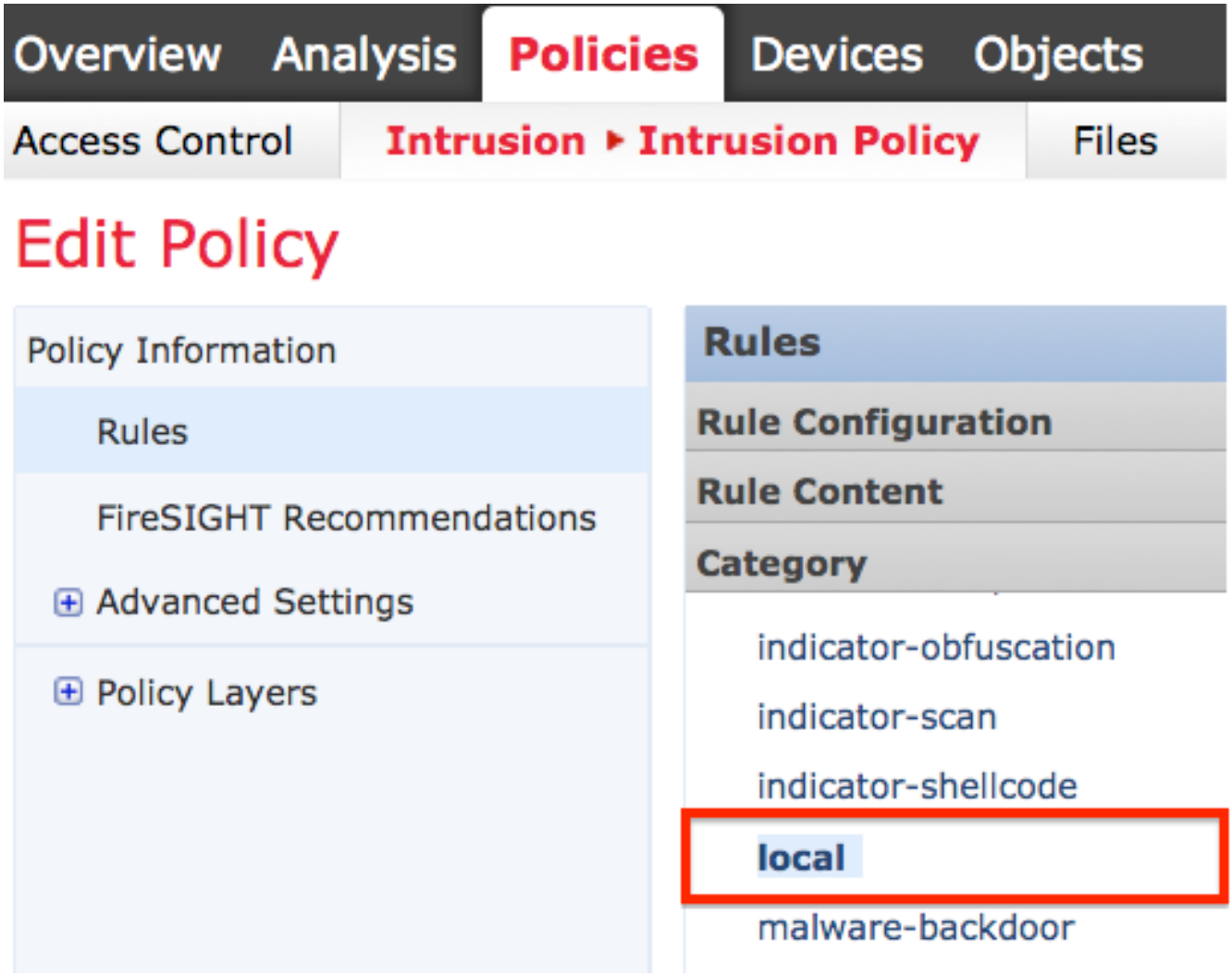
- Um die Revisionsnummer für eine aktuelle lokale Regel anzuzeigen, navigieren Sie zur Seite **Regel-Editor** (**Richtlinien > Intrusion > Regel-Editor**).



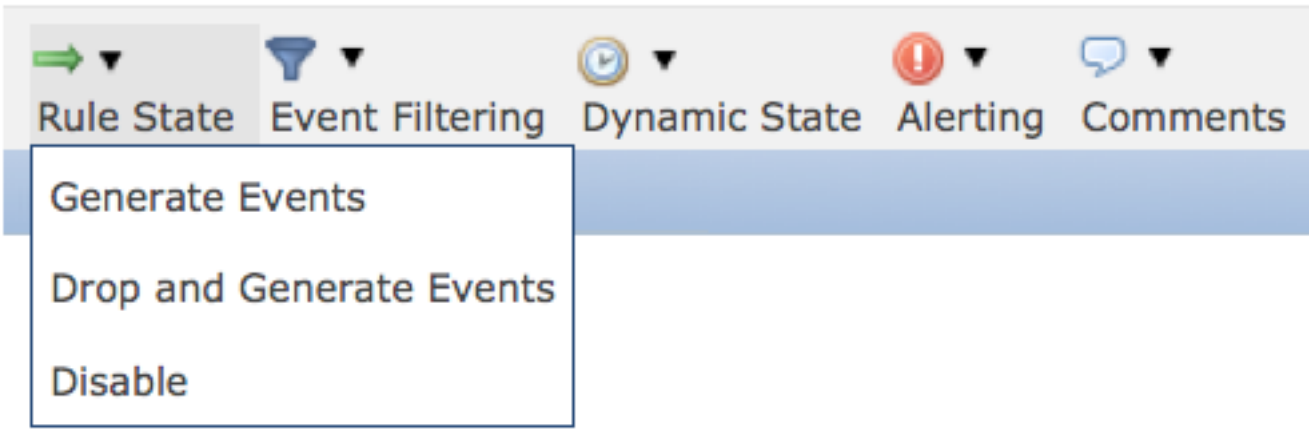
- Klicken Sie auf der Seite Regel-Editor auf die Kategorie **Lokale Regel,** um den Ordner zu erweitern, und klicken Sie dann neben der Regel auf **Bearbeiten**.
- Alle importierten lokalen Regeln werden automatisch in der Kategorie **lokale Regeln** gespeichert.

Lokale Regeln aktivieren

- Standardmäßig setzt das FireSIGHT-System die lokalen Regeln in einen deaktivierten Zustand. Sie müssen den Status der lokalen Regeln manuell festlegen, bevor Sie sie in Ihrer Richtlinie für Sicherheitsrisiken verwenden können.
- Um eine lokale Regel zu aktivieren, navigieren Sie zur Seite "Policy Editor" (**Richtlinien > Intrusion > Intrusion Policy**). Wählen Sie im linken Bereich **Regeln** aus. Wählen Sie unter **Kategorie** die Option **Lokal aus**. Alle lokalen Regeln sollten angezeigt werden, sofern verfügbar.



- Nachdem Sie die gewünschten lokalen Regeln ausgewählt haben, wählen Sie einen Status für die Regeln aus.



- Klicken Sie nach Auswahl des Regelstatus im linken Bereich auf die Option **Policy Information (Richtlinieninformationen)**. Wählen Sie die Schaltfläche **Änderungen bestätigen**. Die Angriffsrichtlinie wird validiert.

Anmerkung: Die Richtlinienvalidierung schlägt fehl, wenn Sie eine importierte lokale Regel aktivieren, die das veraltete threshold-Schlüsselwort in Kombination mit der Grenzwertfunktion für Angriffsereignisse in einer Angriffsrichtlinie verwendet.

Gelöschte lokale Regeln anzeigen

- Alle gelöschten lokalen Regeln werden aus der lokalen Regelkategorie in die gelöschte Regelkategorie verschoben.
- Um die Revisionsnummer einer gelöschten lokalen Regel anzuzeigen, gehen Sie zur Seite **Regel-Editor,** klicken Sie auf die Kategorie, um den Ordner zu erweitern, und klicken Sie dann auf das *Bleistiftsymbol,* um die Details der Regel auf der Seite **Regel-Editor** anzuzeigen.

Nummerierung der lokalen Regeln

- Sie müssen keinen Generator (GID) angeben. Wenn dies der Fall ist, können Sie nur GID 1 für eine Standardtextregel oder 138 für eine Regel für vertrauliche Daten angeben.
- Geben Sie beim erstmaligen Importieren einer Regel keine Snort-ID (SID) oder Revisionsnummer an. Dadurch werden Kollisionen mit SIDs anderer Regeln, einschließlich gelöschter Regeln, vermieden.
- Das FireSIGHT Management Center weist automatisch die nächste verfügbare benutzerdefinierte Regel-SID von 1000000 oder höher und die Revisionsnummer 1 zu.
- Wenn Sie versuchen, eine Angriffsregel mit einer SID größer als 2147483647 zu importieren, tritt ein Validierungsfehler auf.
- Beim Importieren einer aktualisierten Version einer lokalen Regel, die Sie zuvor importiert haben, müssen Sie die von IPS zugewiesene SID und eine Versionsnummer angeben, die größer ist als die aktuelle Versionsnummer.
- Sie können eine von Ihnen gelöschte lokale Regel wiederherstellen, indem Sie die Regel mithilfe der vom IPS zugewiesenen SID und einer Versionsnummer importieren, die größer ist als die aktuelle Versionsnummer. Beachten Sie, dass das FireSIGHT Management Center beim Löschen einer lokalen Regel die Versionsnummer automatisch erhöht. Dies ist ein Gerät, mit dem Sie lokale Regeln wiederherstellen können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.