Filtern von Snort-Regeln basierend auf der SRU- und LSP-Version von FirePOWER-Geräten, die von FMC verwaltet werden

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Snort-Regeln basierend auf der Cisco Secure Rule Update (SRU)- und Link State Packet (LSP)-Version von Firepower-Geräten gefiltert werden, die vom FirePOWER Management Center (FMC) verwaltet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von Open-Source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieser Artikel gilt für alle Firepower-Plattformen.
- Cisco Firepower Threat Defense (FTD) mit der Softwareversion 7.0.0
- FirePOWER Management Center Virtual (FMC) mit der Softwareversion 7.0.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

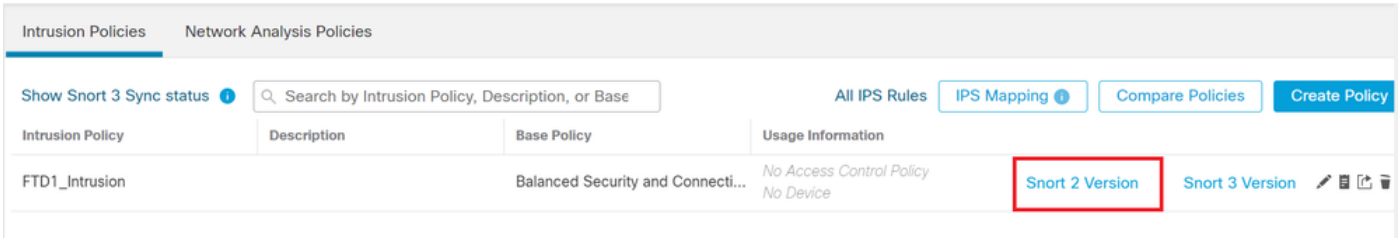
Im Kontext von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) steht "SID" für "Signature ID" oder "Snort Signature ID".

Eine Snort Signature ID (SID) ist eine eindeutige ID, die jeder Regel oder Signatur innerhalb ihres Regelsatzes zugewiesen wird. Diese Regeln werden verwendet, um bestimmte Muster oder Verhaltensweisen im Netzwerkverkehr zu erkennen, die auf schädliche Aktivitäten oder Sicherheitsbedrohungen hinweisen können. Jede Regel ist mit einer SID verknüpft, um den Zugriff und die Verwaltung zu vereinfachen.

Weitere Informationen zu Open-Source Snort finden Sie auf der SNORT-Website.

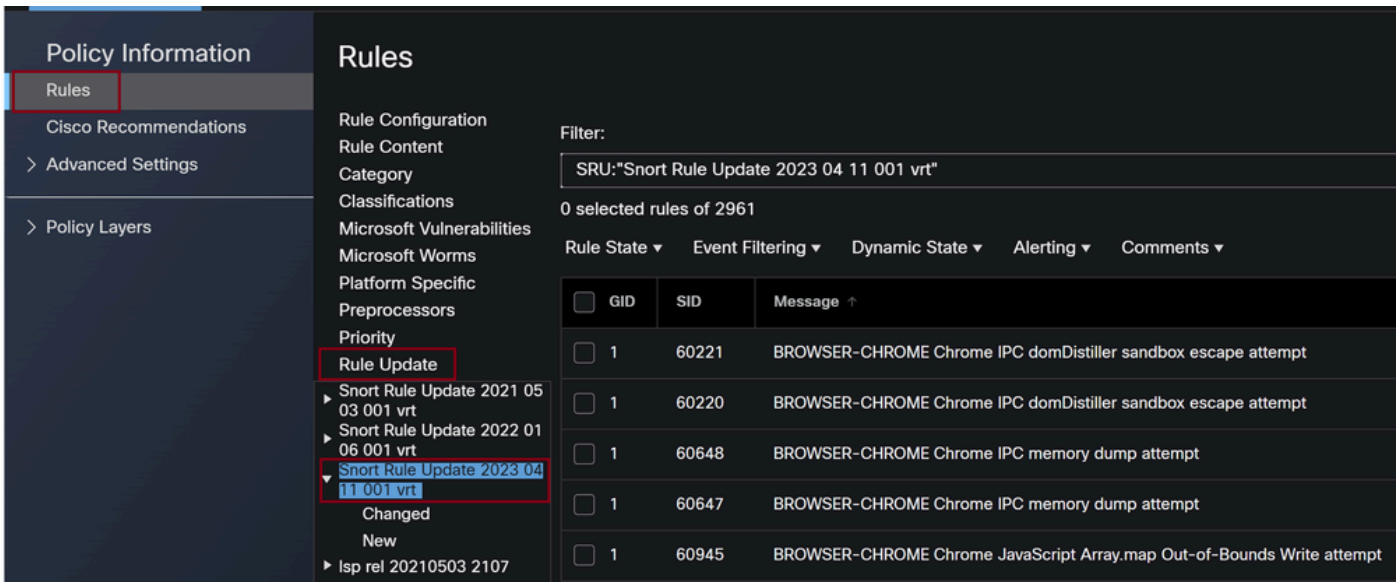
Verfahren zum Filtern von Snort-Regeln

Um die Snort 2-Regel-SIDs anzuzeigen, navigieren Sie zu FMC Policies > Access Control > Intrusion, Klicken Sie anschließend auf die SNORT2-Option in der rechten oberen Ecke, wie im Bild gezeigt:

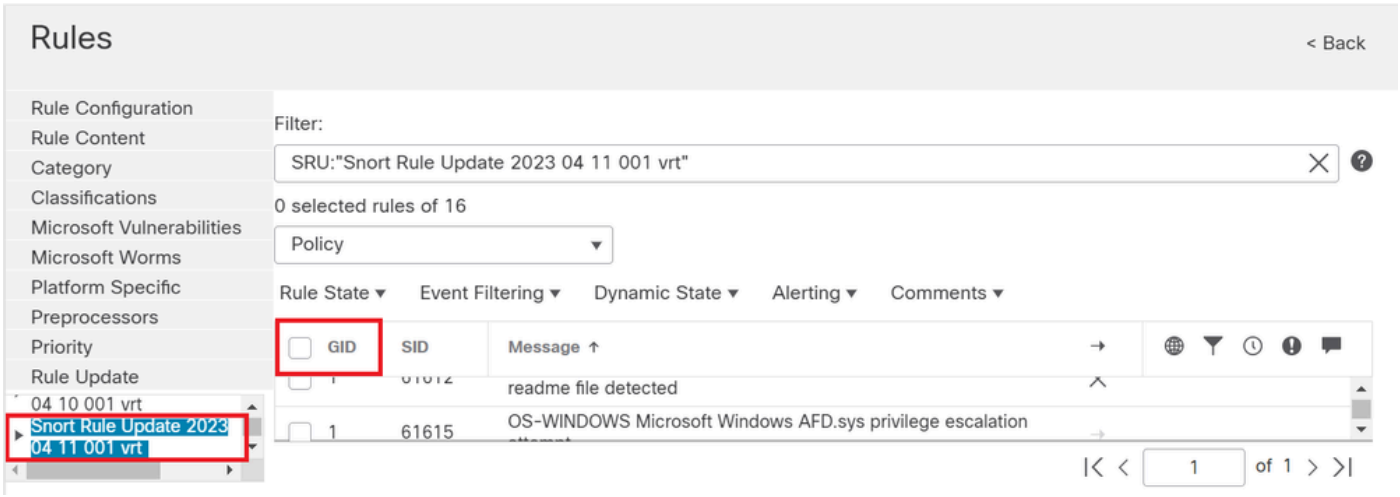


Snort 2

Navigieren Sie zu Rules > Rule Update und wählen Sie das späteste Datum aus, um die SID zu filtern.

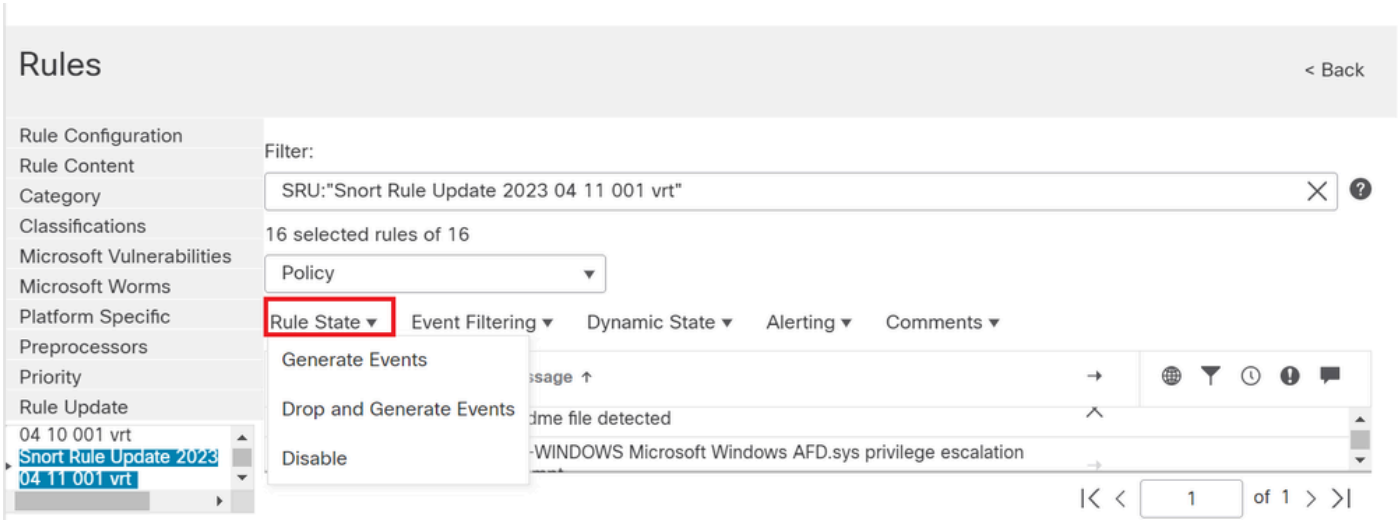


Regelaktualisierung



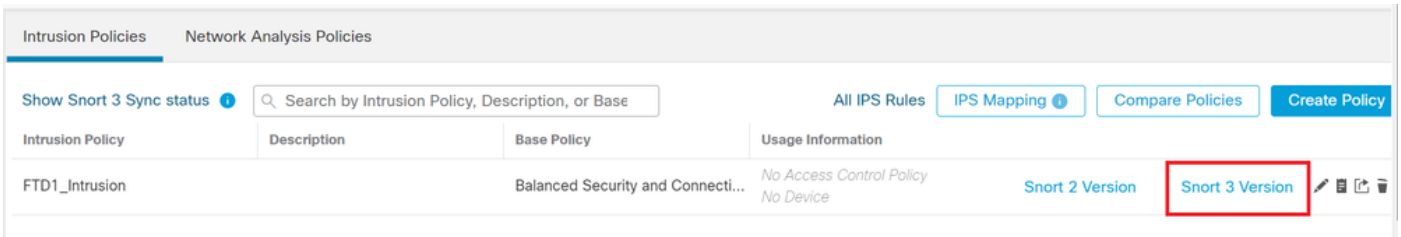
Verfügbare Sids gemäß Snort-Regeln

Wählen Sie die gewünschte Option unter Rule State wie im Bild dargestellt.



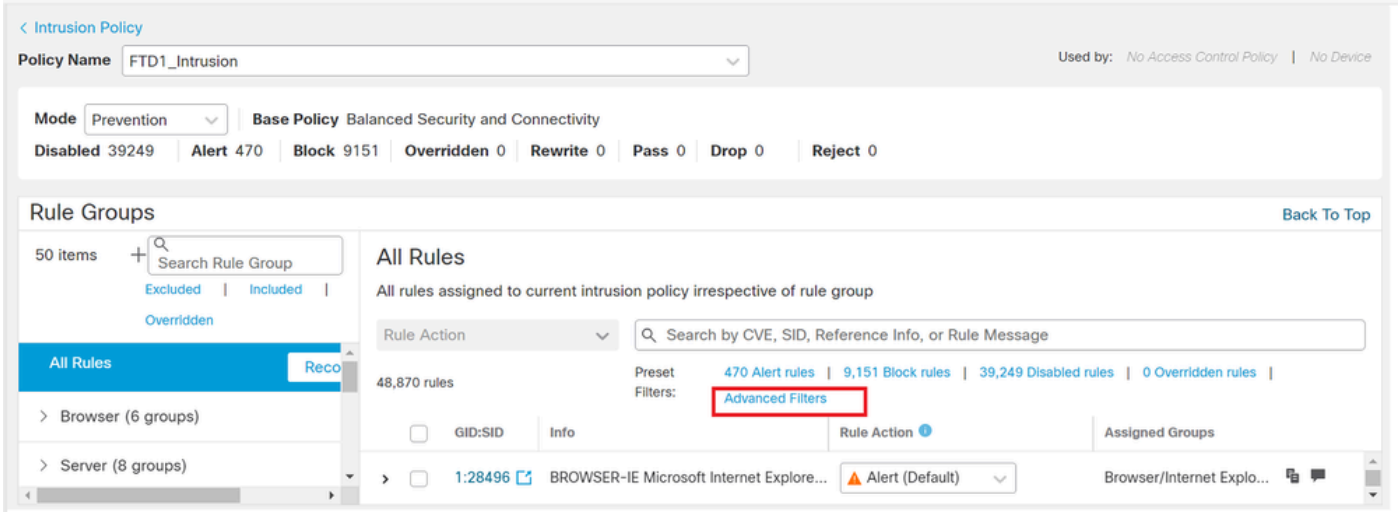
Auswählen von Regelzuständen

Um die Snort 3-Regel-SIDs anzuzeigen, navigieren Sie zu FMC Policies > Access Control > Intrusion , klicken Sie anschließend auf die SNORT3-Option in der rechten oberen Ecke, wie in der Abbildung dargestellt:

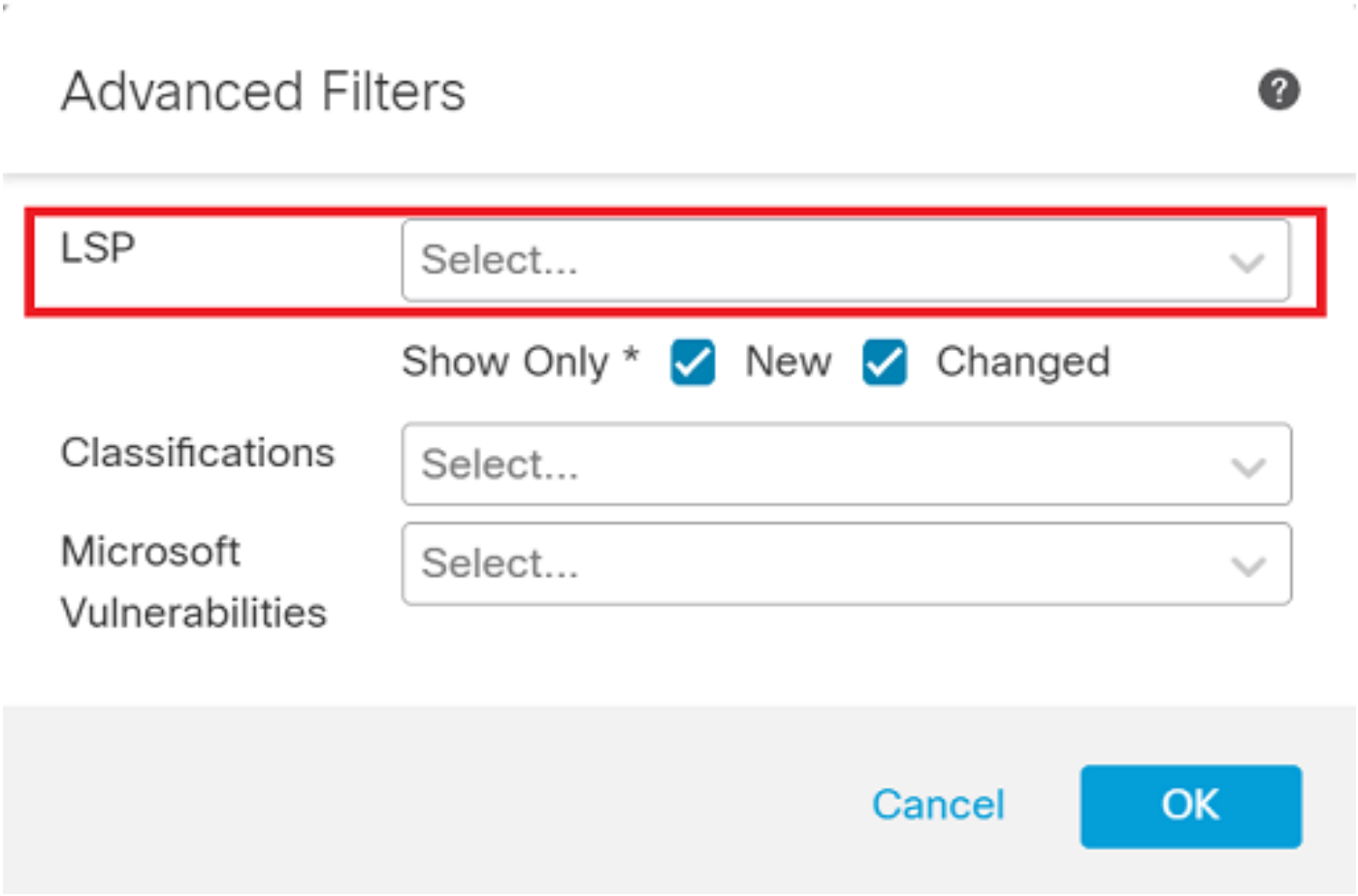


Snort 3

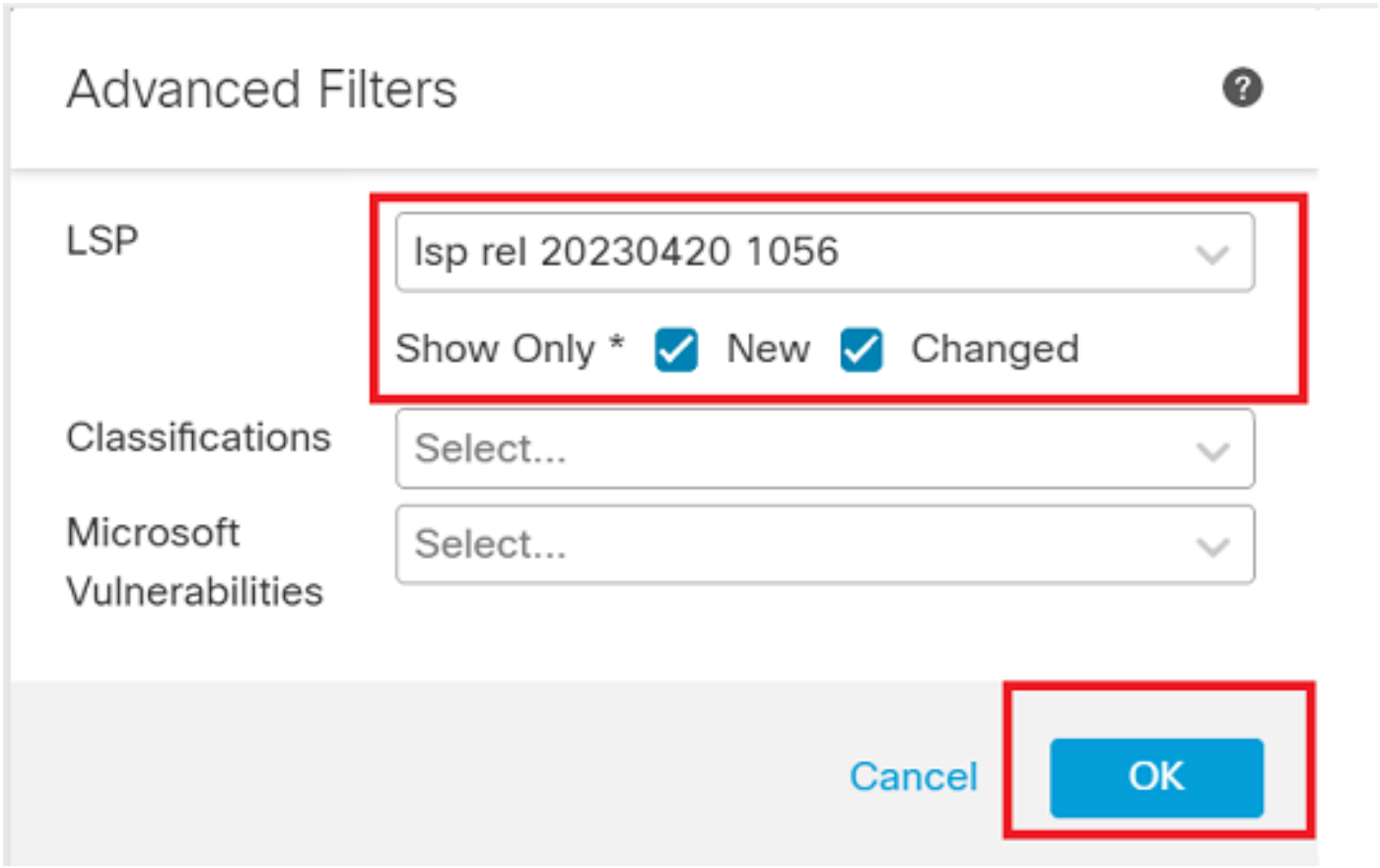
Navigieren Sie zu Advanced Filters und wählen Sie das späteste Datum aus, um die SID wie im Bild dargestellt zu filtern.



Snort 3-Filter



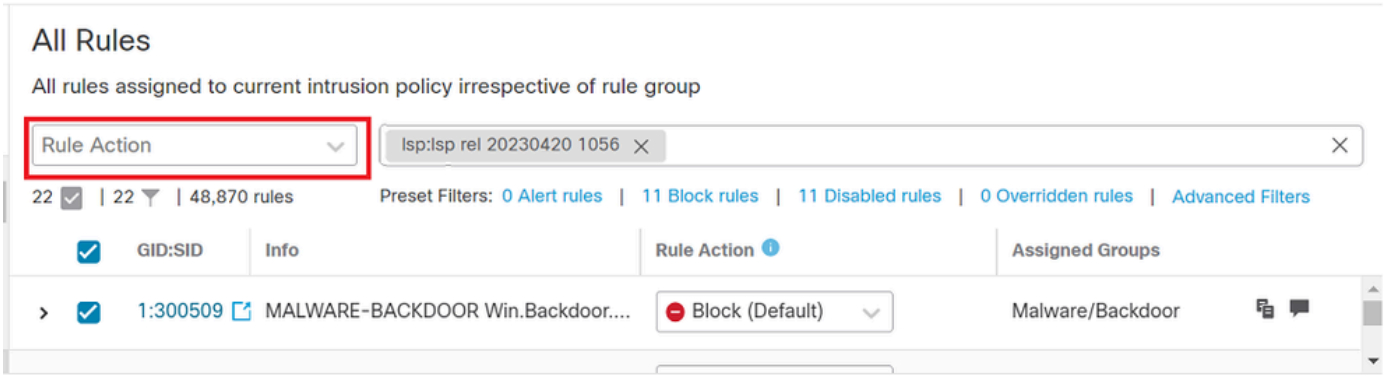
LSP mit erweitertem Filter



LSP-Version

Voreingestellter Filter für Sid's

Wählen Sie die gewünschte Option unter Rule state wie im Bild dargestellt.



Regelaktion

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.