Beispiel für eine URL-Filterung in einem FireSIGHT-System

Inhalt

Einführung

In diesem Dokument werden die Schritte zum Konfigurieren der URL-Filterung auf FireSIGHT System beschrieben. Mit der URL-Filterfunktion im FireSIGHT Management Center können Sie eine Bedingung in eine Zugriffskontrollregel schreiben, um den Datenverkehr, der ein Netzwerk durchläuft, anhand nicht verschlüsselter URL-Anfragen der überwachten Hosts zu bestimmen.

Voraussetzungen

Anforderungen

Dieses Dokument enthält einige spezifische Anforderungen für die URL-Filterungslizenz und den Port.

URL-Filterungslizenz erforderlich

Ein FireSIGHT Management Center benötigt eine URL-Filterungslizenz, um regelmäßig mit der Cloud Kontakt aufnehmen zu können, um die URL-Informationen aktualisieren zu können. Sie können den Zugriffskontrollregeln ohne URL-Filterungslizenz Kategorie- und reputationsbasierte URL-Bedingungen hinzufügen. Sie können die Zugriffskontrollrichtlinie jedoch erst anwenden, wenn Sie dem FireSIGHT Management Center eine URL-Filterungslizenz hinzufügen und diese dann auf den Geräten aktivieren, die von der Richtlinie betroffen sind.

Wenn eine URL-Filterungslizenz abläuft, stoppen Zugriffskontrollregeln mit Kategorie- und reputationsbasierten URL-Bedingungen die Filterung von URLs, und das FireSIGHT Management Center kontaktiert den Cloud-Service nicht mehr. Ohne eine URL-Filterungslizenz können

einzelne URLs oder Gruppen von URLs auf Zulassen oder Blockieren festgelegt werden. Die URL-Kategorie oder Reputationsdaten können jedoch nicht zum Filtern des Netzwerkverkehrs verwendet werden.

Port-Anforderung

Ein FireSIGHT-System verwendet die Ports 443/HTTPS und 80/HTTP, um mit dem Cloud-Service zu kommunizieren. Port 443/HTTPS muss bidirektional geöffnet werden, und der eingehende Zugriff auf Port 80/HTTP muss im FireSIGHT Management Center zugelassen werden.

Verwendete Komponenten

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

- FirePOWER-Appliances: Serie 7000, Serie 8000
- Next Generation Intrusion Prevention System (NGIPS) Virtual Appliance
- Adaptive Security Appliance (ASA) FirePOWER
- Sourcefire Software Version 5.2 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

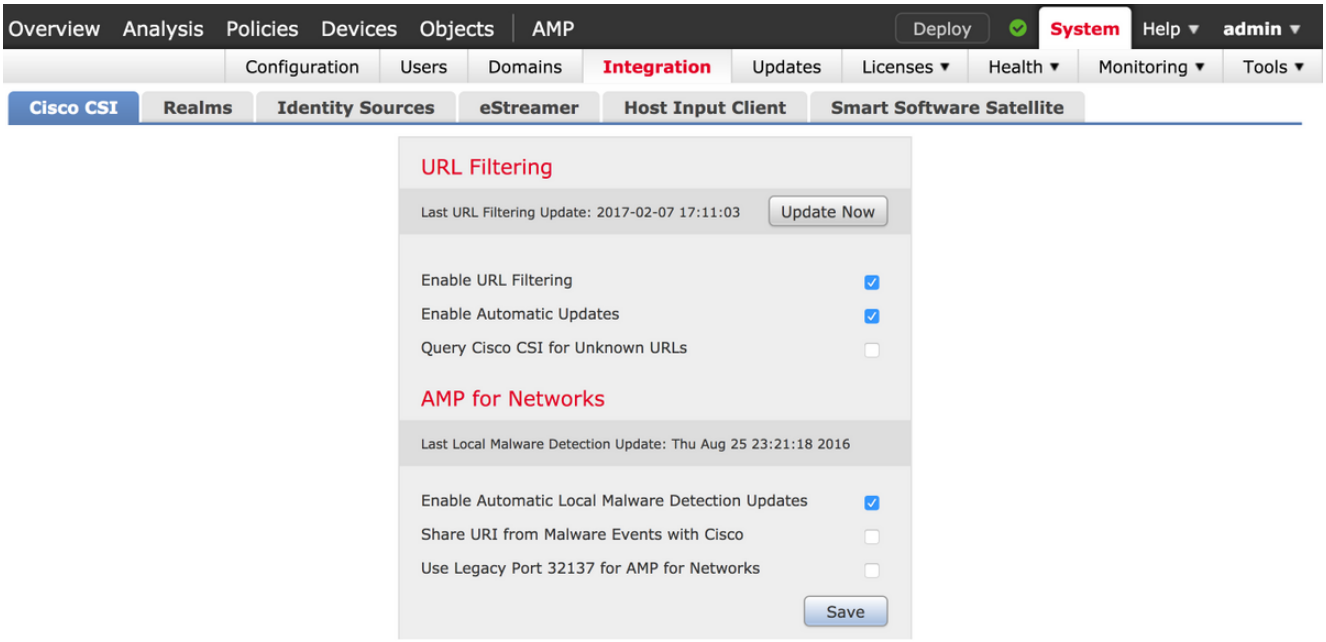
URL-Filterung im FireSIGHT Management Center aktivieren

Gehen Sie wie folgt vor, um die URL-Filterung zu aktivieren:

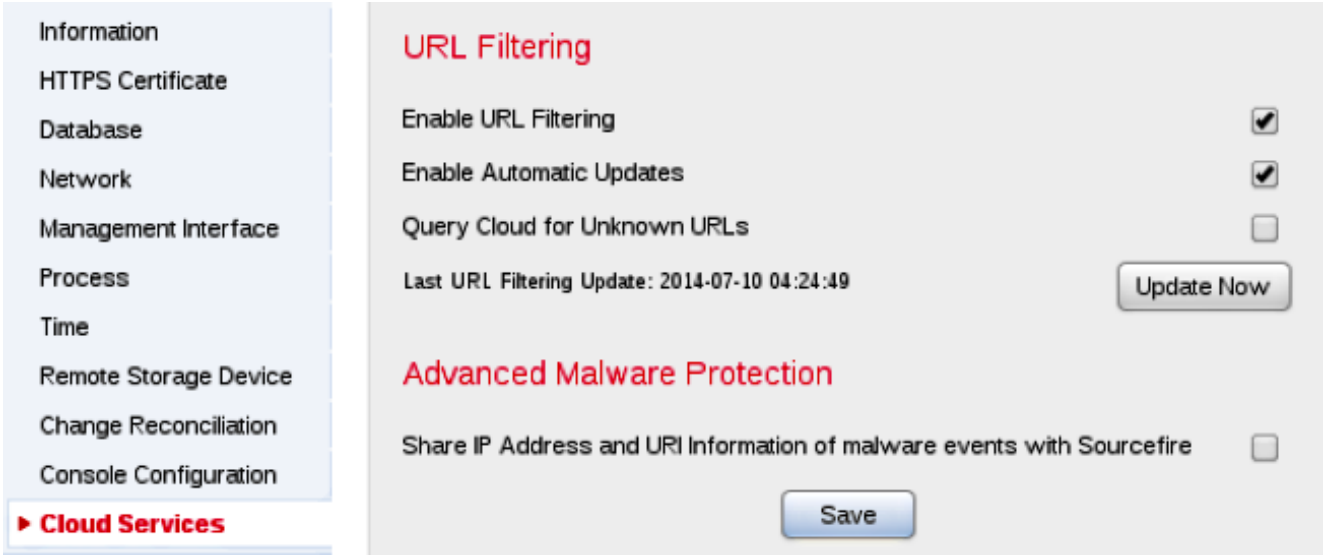
1. Melden Sie sich bei der Web-Benutzeroberfläche des FireSIGHT Management Center an.

2. Die Navigation unterscheidet sich je nach der verwendeten Softwareversion:

   Wählen Sie in Version 6.1.x **System > Integration > Cisco CSI aus**.



Wählen Sie in Version 5.x **System > Local > Configuration aus**. Wählen Sie **Cloud-Services**.



3. Aktivieren Sie das Kontrollkästchen **URL-Filterung aktivieren**, um die URL-Filterung zu aktivieren.
4. Aktivieren Sie ggf. das Kontrollkästchen **Automatische Updates aktivieren**, um automatische Updates zu aktivieren. Diese Option ermöglicht dem System, sich regelmäßig an den Cloud-Service zu wenden, um Aktualisierungen der URL-Daten in den lokalen Datensätzen der Appliance zu erhalten.

   Hinweis: Obwohl der Cloud-Service seine Daten in der Regel einmal pro Tag aktualisiert, muss das FireSIGHT Management Center automatisch alle 30 Minuten überprüfen, um sicherzustellen, dass die Informationen stets aktuell sind. Auch wenn tägliche Updates tendenziell klein sind, können neue URL-Filterungsdaten bis zu 20 Minuten in Anspruch nehmen, wenn sie seit dem letzten Update mehr als fünf Tage vergangen sind. Wenn die Updates heruntergeladen wurden, kann es bis zu 30 Minuten dauern, bis das Update selbst durchgeführt wird.

5. Aktivieren Sie ggf. das Kontrollkästchen **Query Cloud for Unknown URLs** for Unknown URLs (Cloud-Abfrage für unbekannte URLs **abfragen**), um den Cloud-Service für unbekannte URLs

abzufragen. Mit dieser Option kann das System die Sourcefire-Cloud abfragen, wenn jemand in Ihrem überwachten Netzwerk versucht, eine URL aufzurufen, die sich nicht im lokalen Datensatz befindet. Wenn die Cloud die Kategorie oder Reputation einer URL nicht kennt oder das FireSIGHT Management Center keine Verbindung zur Cloud herstellen kann, stimmt die URL die Zugriffskontrollregeln nicht mit Kategorie- oder reputationsbasierten URL-Bedingungen überein.

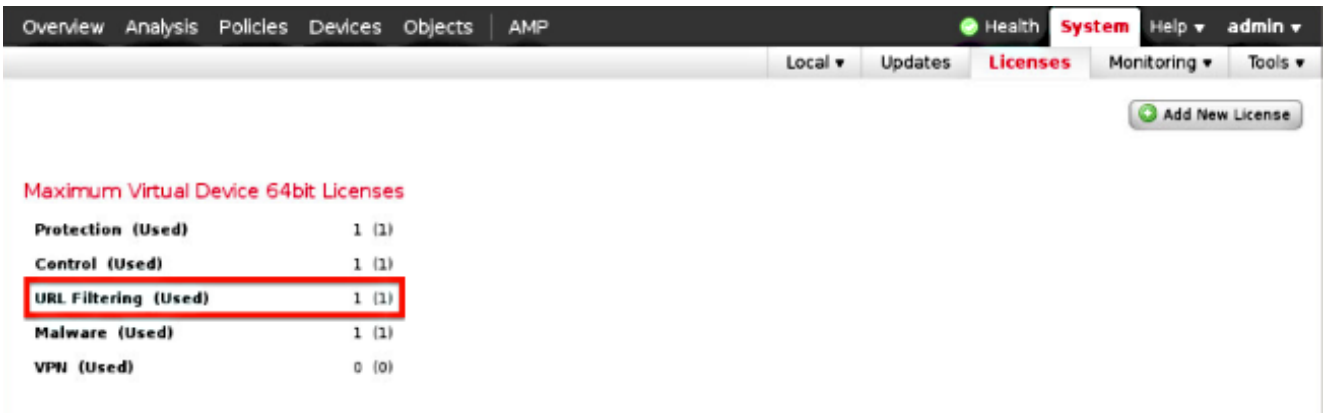
Hinweis: Sie können URLs keine Kategorien oder Reputationen manuell zuweisen. Deaktivieren Sie diese Option, wenn Sie beispielsweise aus Datenschutzgründen nicht möchten, dass Ihre nicht kategorisierten URLs von der Sourcefire-Cloud katalogisiert werden.

6. Klicken Sie auf **Speichern**. URL-Filterungseinstellungen werden gespeichert.

   Hinweis: Wenn Sie die URL-Filterung zum ersten Mal aktiviert haben, ruft ein FireSIGHT Management Center die URL-Filterungsdaten aus dem Cloud-Dienst ab, und zwar basierend auf der Dauer seit der letzten Aktivierung der URL-Filterung.

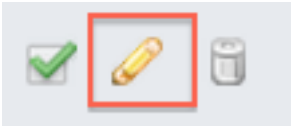
URL-Filterungslizenz auf einem verwalteten Gerät anwenden

1. Überprüfen Sie, ob die URL-Filterungslizenz im FireSIGHT Management Center installiert ist. Öffnen Sie die Seite **System > Lizenzen**, um eine Liste der Lizenzen anzuzeigen.

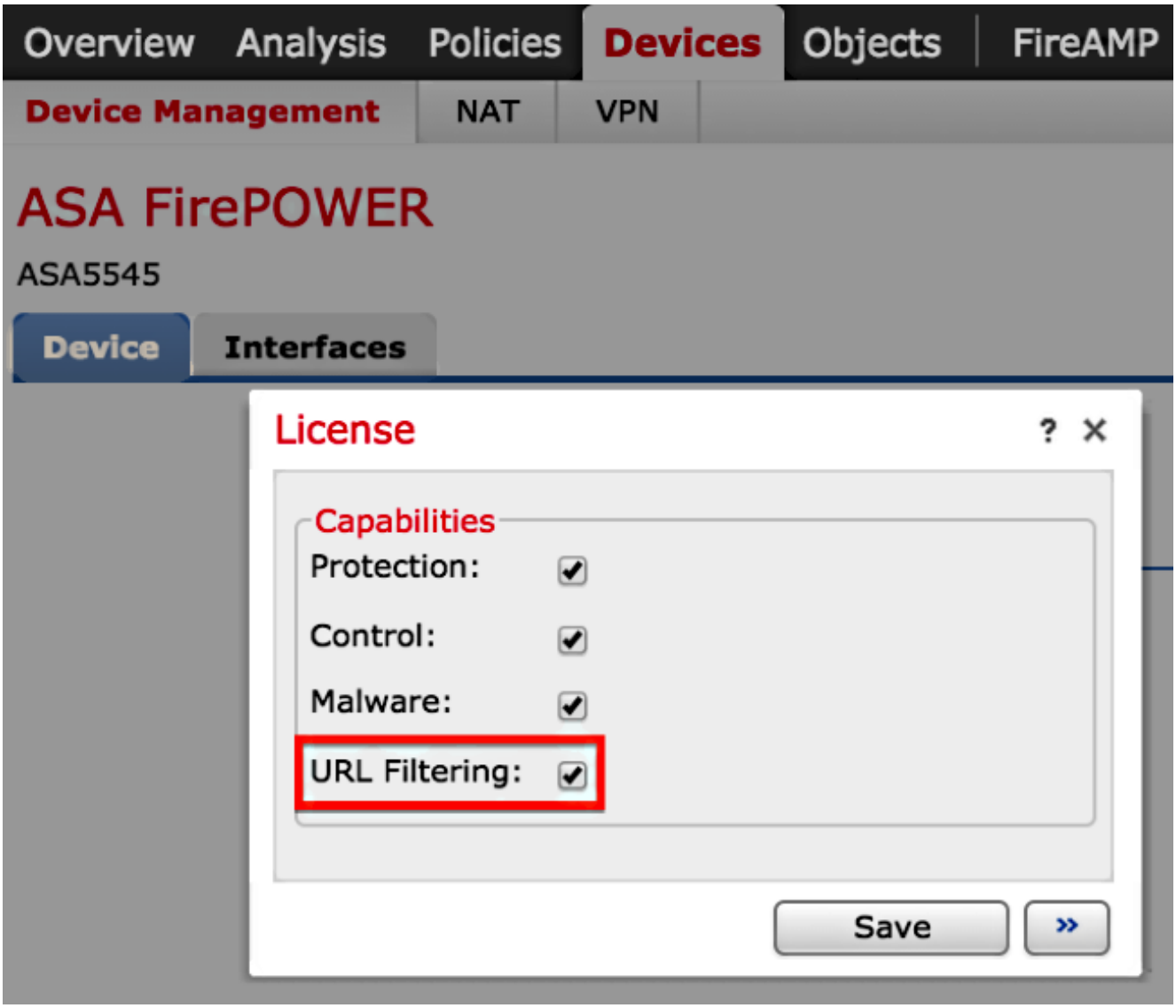


2. Öffnen Sie die Seite **Geräte > Gerätemanagement**, und überprüfen Sie, ob die URL-Filterungslizenz auf das Gerät angewendet wird, das den Datenverkehr überwacht.

3. Wenn die URL-Filterungslizenz nicht auf ein Gerät angewendet wird, klicken Sie auf das **Bleistiftsymbol**, um die Einstellungen zu bearbeiten. Das Symbol befindet sich neben dem Gerätenamen.



4. Sie können die URL-Filterungslizenz auf einem Gerät über die Registerkarte **Geräte** aktivieren.



5. Nachdem Sie eine Lizenz aktiviert und Ihre Änderungen gespeichert haben, müssen Sie auch auf **Änderungen übernehmen** klicken, um die Lizenz auf das verwaltete Gerät anzuwenden.

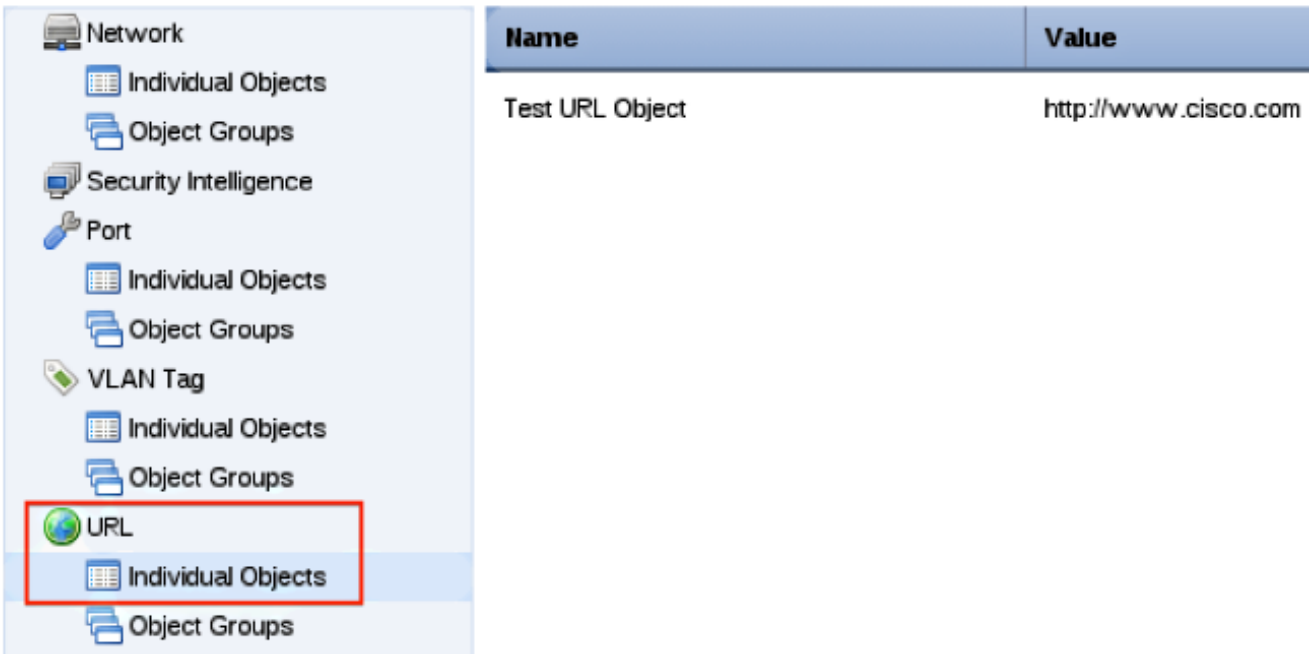
Ausschluss einer bestimmten Site aus einer blockierten URL-Kategorie

FireSIGHT Management Center ermöglicht keine lokale Bewertung von URLs, die die von Sourcefire bereitgestellten Standardkategorien überschreiben. Um diese Aufgabe ausführen zu

können, müssen Sie eine Zugriffskontrollrichtlinie verwenden. In diesen Anweisungen wird beschrieben, wie ein URL-Objekt in einer Zugriffskontrollregel verwendet wird, um eine bestimmte Site von einer Blockkategorie auszuschließen.

1. Öffnen Sie die Seite **Objekte > Objektmanagement**.

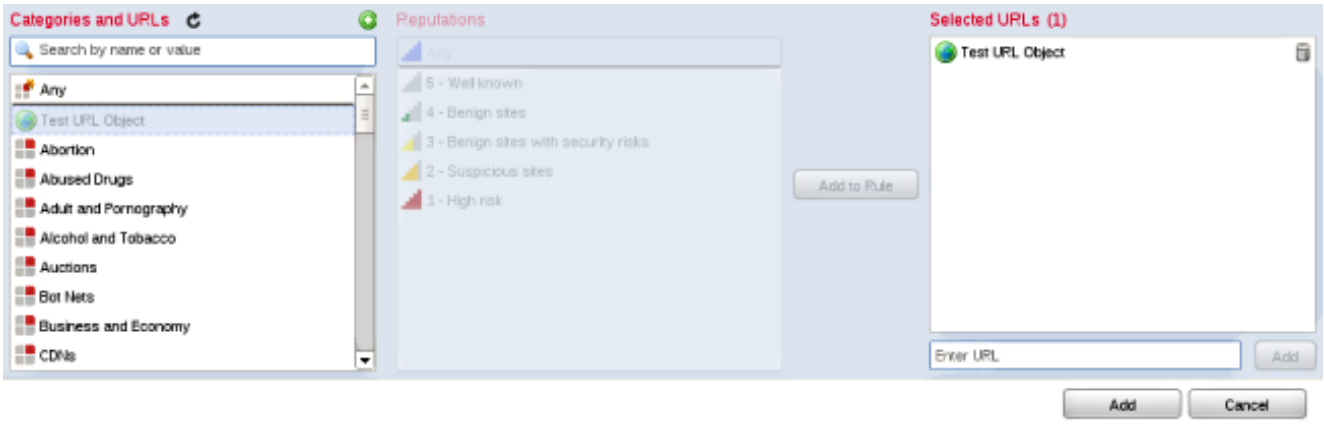
2. **Wählen Sie Individuelle Objekte** als URL aus, und klicken Sie auf die Schaltfläche **URL hinzufügen**. Das Fenster **URL-Objekte** wird angezeigt.



3. Nachdem Sie die Änderungen gespeichert haben, wählen Sie **Richtlinien > Zugriffskontrolle** und klicken Sie auf das **Bleistiftsymbol**, um die Zugriffskontrollrichtlinie zu bearbeiten.

4. Klicken Sie auf **Regel hinzufügen**.

5. Fügen Sie das URL-Objekt der Regel mit der Aktion **Zulassen hinzu** und platzieren Sie es über der URL-Kategorieregel, sodass die Regelaktion zuerst ausgewertet wird.



6. Nachdem Sie die Regel hinzugefügt haben, klicken Sie auf **Speichern und Übernehmen**. Sie speichert die neuen Änderungen und wendet die Zugriffskontrollrichtlinie auf verwaltete Appliances an.

Überprüfen

Informationen zur Überprüfung oder Fehlerbehebung finden Sie im Artikel **Troubleshoot Issues with URL Filtering on FireSIGHT System (Fehlerbehebung bei URL-Filterung auf FireSIGHT-System)** im Abschnitt "Related Information" (Zugehörige Informationen).

Fehlerbehebung

Informationen zur Überprüfung oder Fehlerbehebung finden Sie im **Fehlerbehebung bei URL-Filterung im FireSIGHT-System** im Abschnitt "Zugehörige Informationen" verlinkt.

Zugehörige Informationen

- Fehlerbehebung bei URL-Filterung im FireSIGHT-System
- Technischer Support und Dokumentation - Cisco Systems