

URL-Filterung in einem FireSIGHT-System - Konfigurationsbeispiel

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[URL-Filterungslizenz erforderlich](#)

[Port-Anforderung](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[URL-Filterung in FireSIGHT Management Center aktivieren](#)

[Anwendung der URL-Filterungslizenz auf einem verwalteten Gerät](#)

[Ausschluss einer bestimmten Site aus der Kategorie der gesperrten URLs](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der URL-Filterung auf dem FireSIGHT-System beschrieben. Mit der URL-Filterfunktion des FireSIGHT Management Center können Sie eine Bedingung in eine Zugriffskontrollregel schreiben, um den Datenverkehr, der ein Netzwerk durchläuft, auf der Grundlage nicht verschlüsselter URL-Anforderungen 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-Filterlizenz, um sich regelmäßig an die Cloud zu wenden und URL-Informationen zu aktualisieren. Sie können kategoriebasierte und reputationsbasierte URL-Bedingungen zu Zugriffskontrollregeln ohne URL-Filterungslizenz hinzufügen. Sie können die Zugriffskontrollrichtlinie jedoch erst anwenden, wenn Sie dem FireSIGHT Management Center eine URL-Filterungslizenz hinzufügen und sie dann auf den von der Richtlinie betroffenen Geräten aktivieren.

Wenn eine URL-Filterungslizenz abläuft, stoppen Zugriffskontrollregeln mit kategorie- und reputationsbasierten URL-Bedingungen das Filtern von URLs, und das FireSIGHT Management

Center kontaktiert den Cloud-Service nicht mehr. Ohne eine URL-Filterungslizenz können einzelne URLs oder Gruppen von URLs so festgelegt werden, dass sie zugelassen oder blockiert 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 folgenden Hardware- und Software-Versionen:

- FirePOWER-Appliances: Serie 7000, Serie 8000
- NGIPS (Intrusion Prevention System) - virtuelle Appliance der nächsten Generation
- Adaptive Security Appliance (ASA) mit FirePOWER
- Sourcefire Softwareversion 5.2 oder höher

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

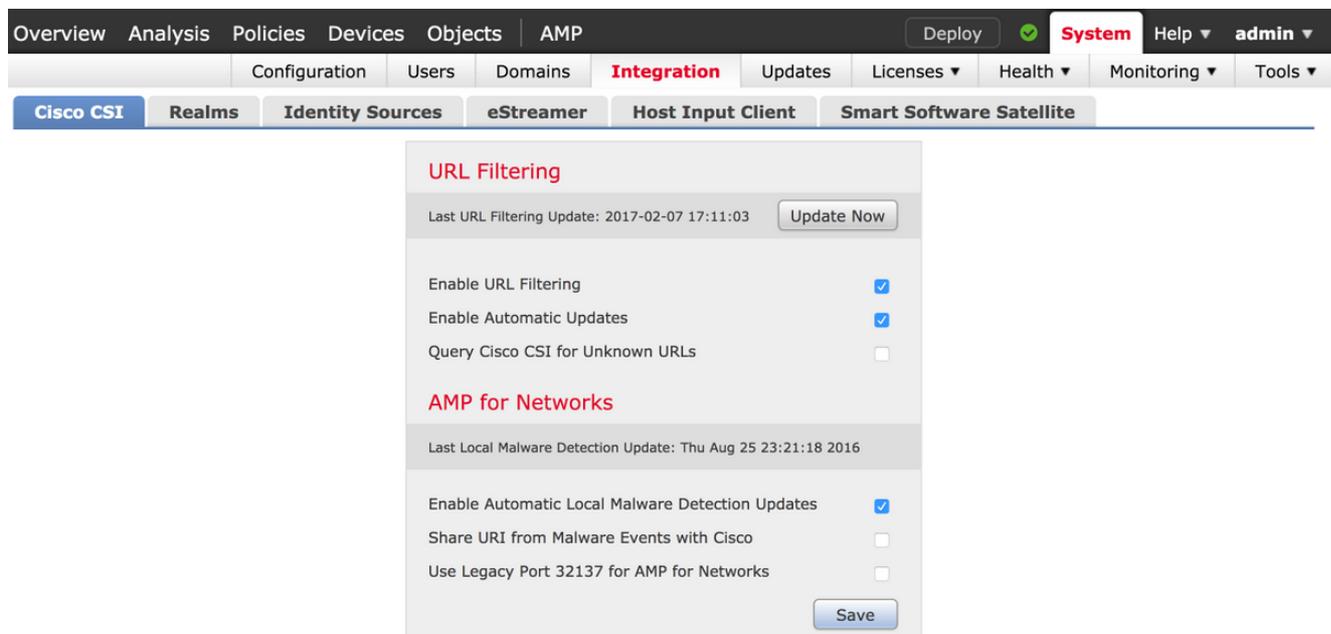
Konfigurieren

URL-Filterung in FireSIGHT Management Center aktivieren

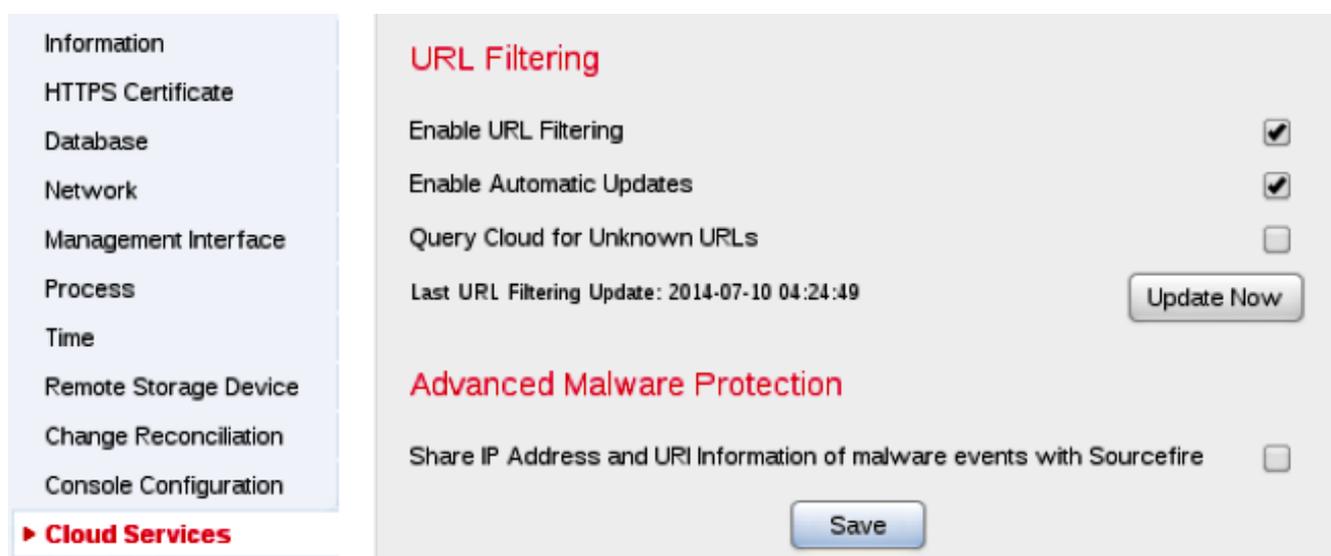
Führen Sie die folgenden Schritte aus, um die URL-Filterung zu aktivieren:

1. Melden Sie sich bei der Web-Benutzeroberfläche des FireSIGHT Management Center an.
2. Die Navigation hängt von der jeweils ausgeführten Softwareversion ab:

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 optional das Kontrollkästchen **Automatische Updates aktivieren**, um automatische Updates zu aktivieren. Mit dieser Option kann das System den Cloud-Service regelmäßig kontaktieren, um Updates für die URL-Daten in den lokalen Datensätzen der Appliance zu erhalten.

Anmerkung: Obwohl der Cloud-Service seine Daten in der Regel einmal täglich aktualisiert, muss das FireSIGHT Management Center bei Aktivierung automatischer Updates alle 30 Minuten eine Überprüfung durchführen, um sicherzustellen, dass die Informationen stets aktuell sind. Auch wenn die täglichen Updates in der Regel klein sind, kann es, wenn es seit dem letzten Update mehr als fünf Tage her ist, bis zum Herunterladen neuer URL-Filterdaten bis zu 20 Minuten dauern. Nach dem Herunterladen der Updates kann es bis zu 30 Minuten dauern, bis die Aktualisierung selbst durchgeführt wird.

5. Aktivieren Sie optional das Kontrollkästchen **Query Cloud for Unknown URLs** for Unknown URLs (Unbekannte URLs abfragen), um den Cloud-Service nach unbekanntem URLs

abzufragen. Mit dieser Option kann das System eine Abfrage an die Sourcefire-Cloud senden, wenn ein Mitarbeiter im überwachten Netzwerk versucht, eine URL zu suchen, die nicht im lokalen Datensatz enthalten ist. 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 den Zugriffskontrollregeln nicht mit den kategorie- oder reputationsbasierten URL-Bedingungen überein.

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

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

Anmerkung: Basierend auf dem Zeitraum seit der letzten Aktivierung der URL-Filterung bzw. wenn Sie die URL-Filterung zum ersten Mal aktiviert haben, ruft ein FireSIGHT Management Center die URL-Filterungsdaten aus dem Cloud-Service ab.

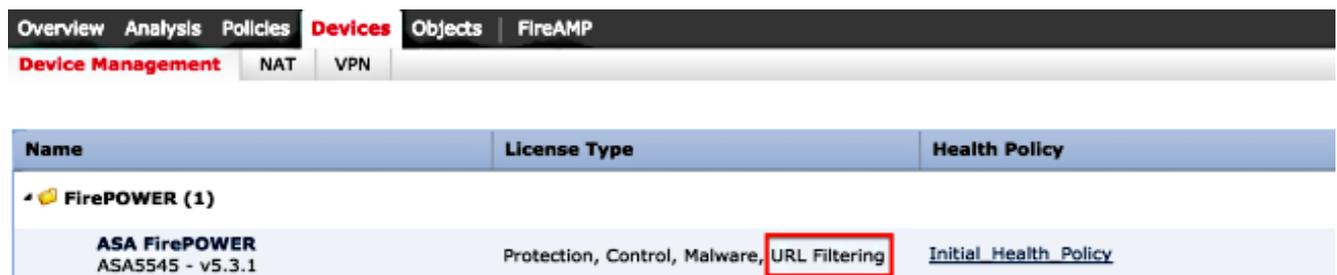
Anwendung der URL-Filterungslizenz auf einem verwalteten Gerät

1. Überprüfen Sie, ob die URL-Filterungslizenz im FireSIGHT Management Center installiert ist. Gehen Sie zur Seite **System > Licenses** (System > Lizenzen), um eine Liste der Lizenzen zu finden.



Maximum Virtual Device 64bit Licenses	
Protection (Used)	1 (1)
Control (Used)	1 (1)
URL Filtering (Used)	1 (1)
Malware (Used)	1 (1)
VPN (Used)	0 (0)

2. Überprüfen Sie auf der Seite **Devices > Device Management (Geräte > Gerätemanagement)**, ob die URL-Filterungslizenz auf das Gerät angewendet wird, das den Datenverkehr überwacht.



Name	License Type	Health Policy
FirePOWER (1)		
ASA FirePOWER ASA5545 - v5.3.1	Protection, Control, Malware, URL Filtering	Initial Health Policy

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.

Overview Analysis Policies **Devices** Objects | FireAMP

Device Management NAT VPN

ASA FirePOWER

ASA5545

Device Interfaces

License ? X

Capabilities

Protection:

Control:

Malware:

URL Filtering:

Save >>

5. Nachdem Sie eine Lizenz aktiviert und die Änderungen gespeichert haben, müssen Sie auch auf **Apply Changes (Änderungen anwenden)** klicken, um die Lizenz auf das verwaltete Gerät anzuwenden.

 **You have unapplied changes**



Ausschluss einer bestimmten Site aus der Kategorie der gesperrten URLs

Das FireSIGHT Management Center lässt keine lokalen URL-Bewertungen zu, die die von

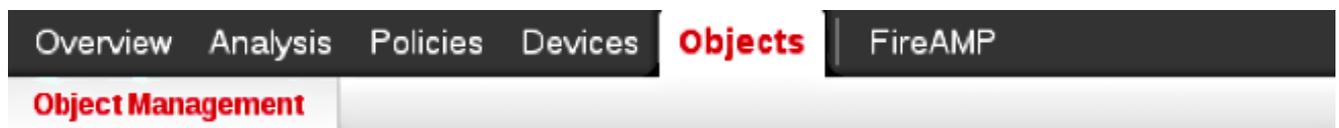
Sourcefire bereitgestellten Standardkategorien überschreiben. Um diese Aufgabe zu erfüllen, müssen Sie eine Zugriffskontrollrichtlinie verwenden. In diesen Anweisungen wird beschrieben, wie ein URL-Objekt in einer Zugriffskontrollregel verwendet wird, um eine bestimmte Site aus einer Blockkategorie auszuschließen.

1. Gehen Sie zur Seite **Objekte > Objektverwaltung**.
2. Wählen Sie **Individuelle Objekte** als URL aus, und klicken Sie auf die Schaltfläche **URL hinzufügen**. Das Fenster **URL-Objekte** wird angezeigt.

URL Objects



Name:	<input type="text" value="Test URL Object"/>
URL:	<input type="text" value="http://www.cisco.com"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	



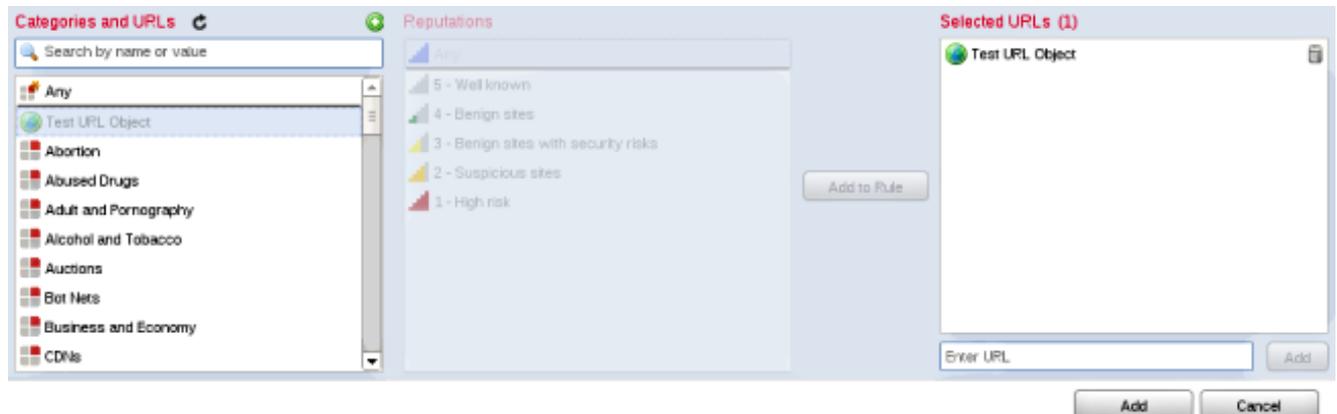
	Name	Value
Network <ul style="list-style-type: none"> Individual Objects Object Groups		
Security Intelligence <ul style="list-style-type: none"> Port<ul style="list-style-type: none"> Individual Objects Object Groups		
VLAN Tag <ul style="list-style-type: none"> Individual Objects Object Groups		
URL <ul style="list-style-type: none"> Individual Objects Object Groups	Test URL Object	http://www.cisco.com

3. Nachdem Sie die Änderungen gespeichert haben, wählen Sie **Policies > Access Control (Richtlinien > Zugriffskontrolle)** aus, und klicken Sie auf das **Bleistiftsymbol**, um die

Zugriffskontrollrichtlinie zu bearbeiten.

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

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



6. Klicken Sie nach dem Hinzufügen der Regel auf **Speichern und anwenden**. Es speichert die neuen Änderungen und wendet die Zugriffskontrollrichtlinie auf verwaltete Appliances an.

Überprüfung

Informationen zum Überprüfen oder Beheben von Problemen finden Sie im Artikel **Fehlerbehebung bei Problemen mit URL-Filterung im FireSIGHT-System**, der im Abschnitt mit den zugehörigen Informationen verknüpft ist.

Fehlerbehebung

Informationen zur Überprüfung oder Fehlerbehebung finden Sie im **Fehlerbehebung bei Problemen mit URL-Filterung auf FireSIGHT-Systemen** Artikel, der im Abschnitt "Verwandte Informationen" verlinkt ist.

Zugehörige Informationen

- [Fehlerbehebung bei Problemen mit URL-Filterung auf FireSIGHT-Systemen](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

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.