Fehlerbehebung bei Problemen mit der URL-Filterung auf einem FireSIGHT-System

Inhalt

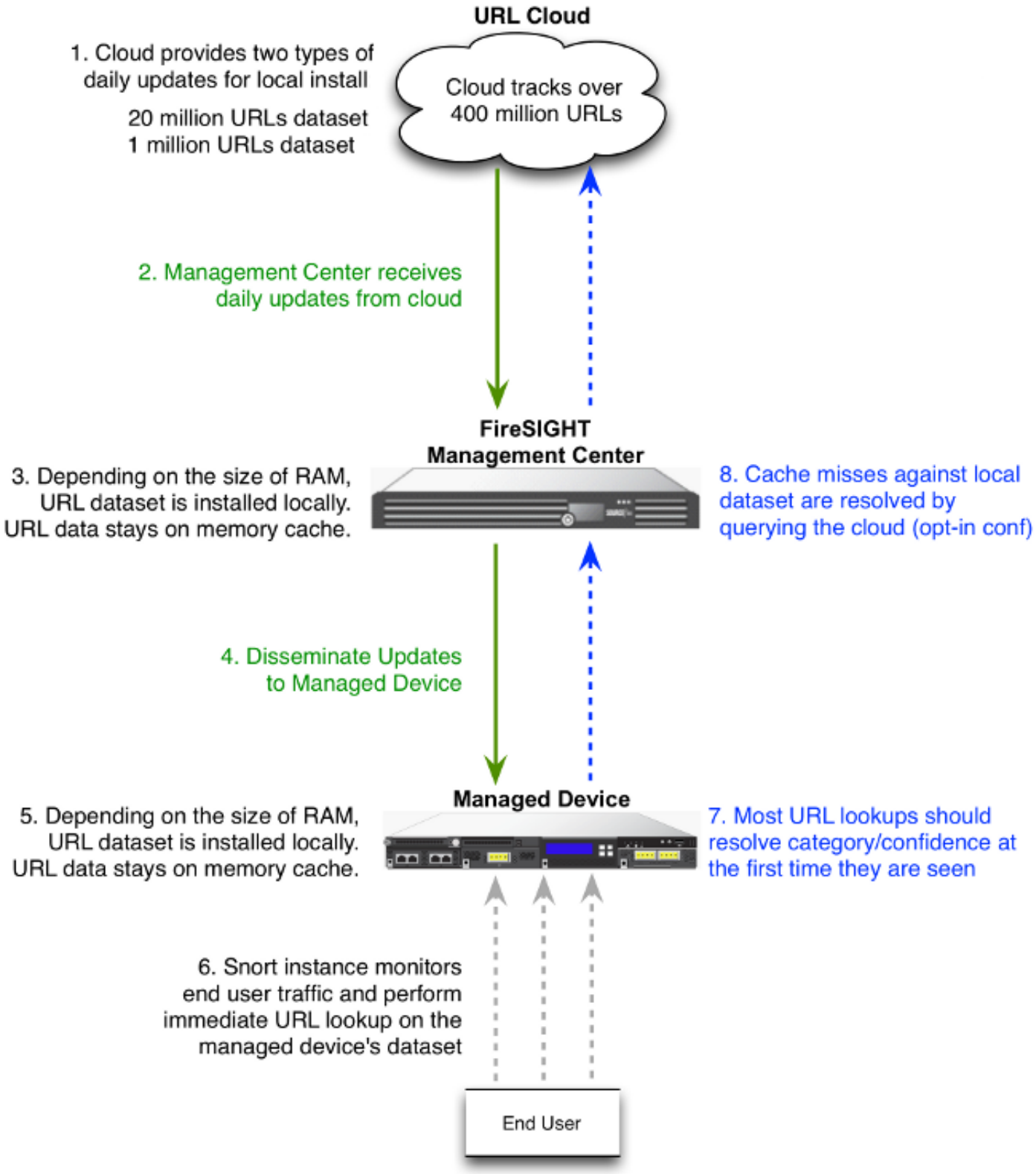
Einleitung

In diesem Dokument werden häufige Probleme bei der URL-Filterung beschrieben. Die URL-Filterfunktion in FireSIGHT Management Center kategorisiert den Datenverkehr von überwachten Hosts und ermöglicht Ihnen, eine Bedingung in eine Zugriffskontrollregel basierend auf der Reputation zu schreiben.

Suchprozess für URL-Filterung

Um die URL-Suche zu beschleunigen, stellt die URL-Filterung ein Dataset bereit, das lokal auf einem FirePOWER-System installiert ist. Je nach verfügbarem Arbeitsspeicher (RAM) auf einer Appliance gibt es zwei Arten von Datensätzen:

Typ des Datasets	Speicheranforderung	
	Auf Version 5.3	Auf Version 5.4 oder höher
20 Millionen URL-Datensätze	>2 GB	>3,4 GB
1 Million URL-Daten	<= 2 GB	<= 3,4 GB



Probleme mit der Cloud-Anbindung

Schritt 1: Lizenzen überprüfen

Ist die Lizenz installiert?

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 zuerst eine URL-Filterungslizenz

hinzufügen und sie dann auf den von der Richtlinie betroffenen Geräten aktivieren.

Ist die Lizenz abgelaufen?

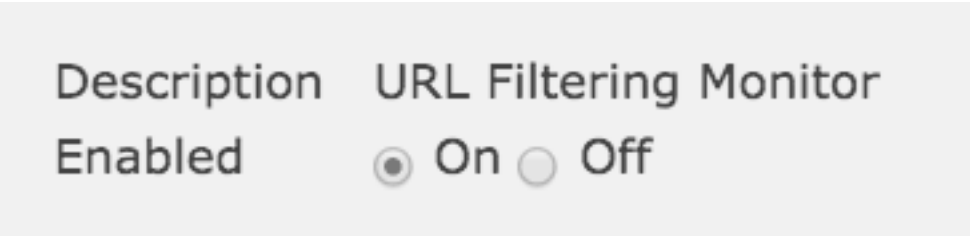
Wenn eine URL-Filterungslizenz abläuft, stoppen Zugriffskontrollregeln mit kategorie- und reputationsbasierten URL-Bedingungen das Filtern von URLs, und das FireSIGHT Management Center kontaktiert den Cloud-Service nicht mehr.

> **Tipp:** Lesen Sie das Konfigurationsbeispiel für die URL-Filterung in einem FireSIGHT-System, um zu erfahren, wie Sie die URL-Filterungsfunktion in einem FireSIGHT-System aktivieren und die URL-Filterungslizenz auf ein verwaltetes Gerät anwenden.

Phase 2: Statusbenachrichtigungen überprüfen

Das Modul "URL-Filterungsmonitor" verfolgt die Kommunikation zwischen dem FireSIGHT Management Center und der Cisco Cloud, wo das System die URL-Filterungsdaten (Kategorie und Reputation) für häufig besuchte URLs abruft. Das Modul "URL-Filterungsmonitor" verfolgt außerdem die Kommunikation zwischen einem FireSIGHT Management Center und allen verwalteten Geräten, auf denen Sie die URL-Filterung aktiviert haben.

Um das Modul "URL-Filterungsmonitor" zu aktivieren, gehen Sie zur Seite **Konfiguration** der **Integritätsrichtlinie**, und wählen Sie **URL-Filterungsmonitor aus**. Klicken Sie auf das Optionsfeld **Ein** für die Option **Aktiviert**, um die Verwendung des Moduls für Statustests zu aktivieren. Sie müssen die Integritätsrichtlinie auf das FireSIGHT Management Center anwenden, wenn Ihre Einstellungen wirksam werden sollen.



- **Kritischer Alarm**: Wenn das FireSIGHT Management Center nicht erfolgreich mit der Cloud kommunizieren oder ein Update aus der Cloud abrufen kann, ändert sich die Statusklassifizierung für dieses Modul in *Kritisch*.
- **Warnmeldung**: Wenn das FireSIGHT Management Center erfolgreich mit der Cloud kommuniziert, ändert sich der Modulstatus in *Warnung,* wenn das Management Center keine neuen URL-Filterungsdaten an seine verwalteten Geräte senden kann.

Schritt 3: DNS-Einstellungen überprüfen

Ein FireSIGHT Management Center kommuniziert bei der Cloud-Suche mit diesen Servern:

```
database.brightcloud.com
service.brightcloud.com
```

Nachdem Sie sichergestellt haben, dass beide Server in der Firewall zugelassen sind, führen Sie die folgenden Befehle im FireSIGHT Management Center aus, und überprüfen Sie, ob das Management Center die Namen auflösen kann:

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

Schritt 4: Überprüfen Sie die Verbindung zu den erforderlichen Ports.

FireSIGHT-Systeme verwenden die Ports 443/HTTPS und 80/HTTP, um mit dem Cloud-Service zu kommunizieren.

Wenn Sie bestätigt haben, dass das Management Center eine erfolgreiche nslookup durchführen kann, überprüfen Sie die Verbindung zu Port 80 und Port 443 mit telnet. Die URL-Datenbank wird mit database.brightcloud.com an Port 443 heruntergeladen, während die unbekannten URL-Abfragen unter service.brightcloud.com an Port 80 durchgeführt werden.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Diese Ausgabe ist ein Beispiel für eine erfolgreiche Telnet-Verbindung mit database.brightcloud.com.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

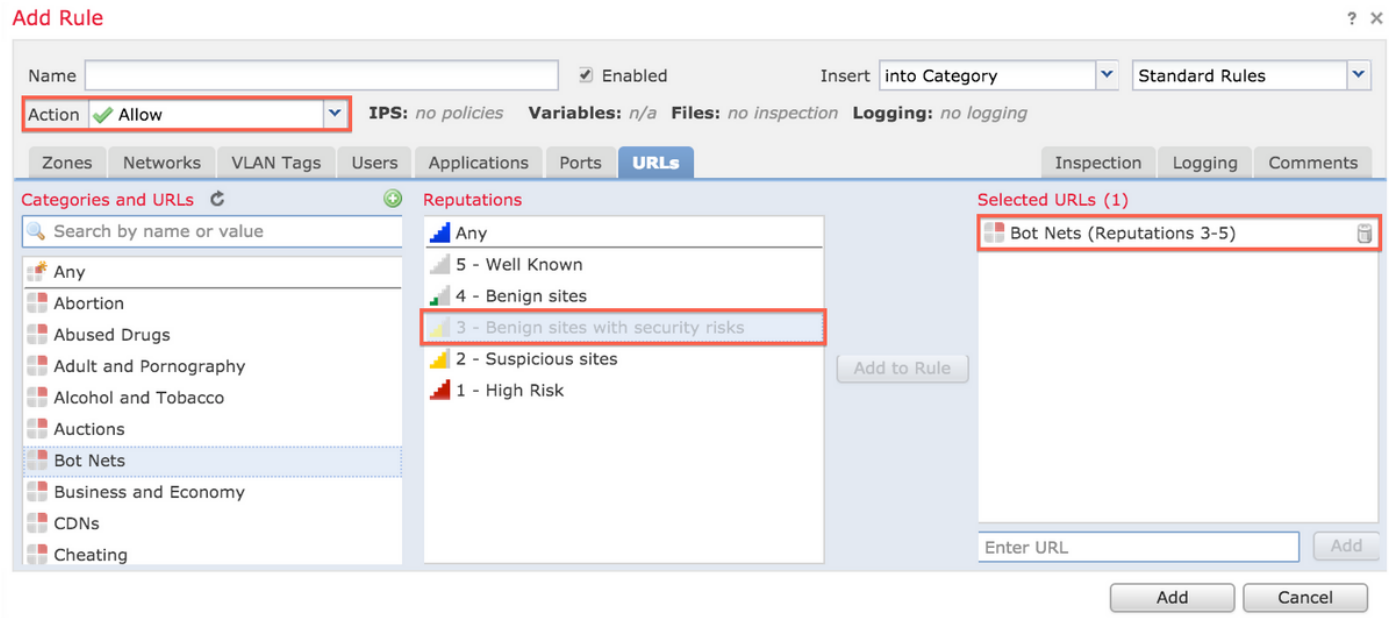
Zugriffskontrolle und Probleme mit falschen Kategorien

Problem 1: URL mit nicht ausgewählter Reputationsstufe ist zulässig/gesperrt

Wenn Sie feststellen, dass eine URL zulässig oder blockiert ist, aber nicht die Reputationsstufe dieser URL in Ihrer Zugriffskontrollregel ausgewählt haben, lesen Sie diesen Abschnitt, um zu erfahren, wie eine URL-Filterregel funktioniert.

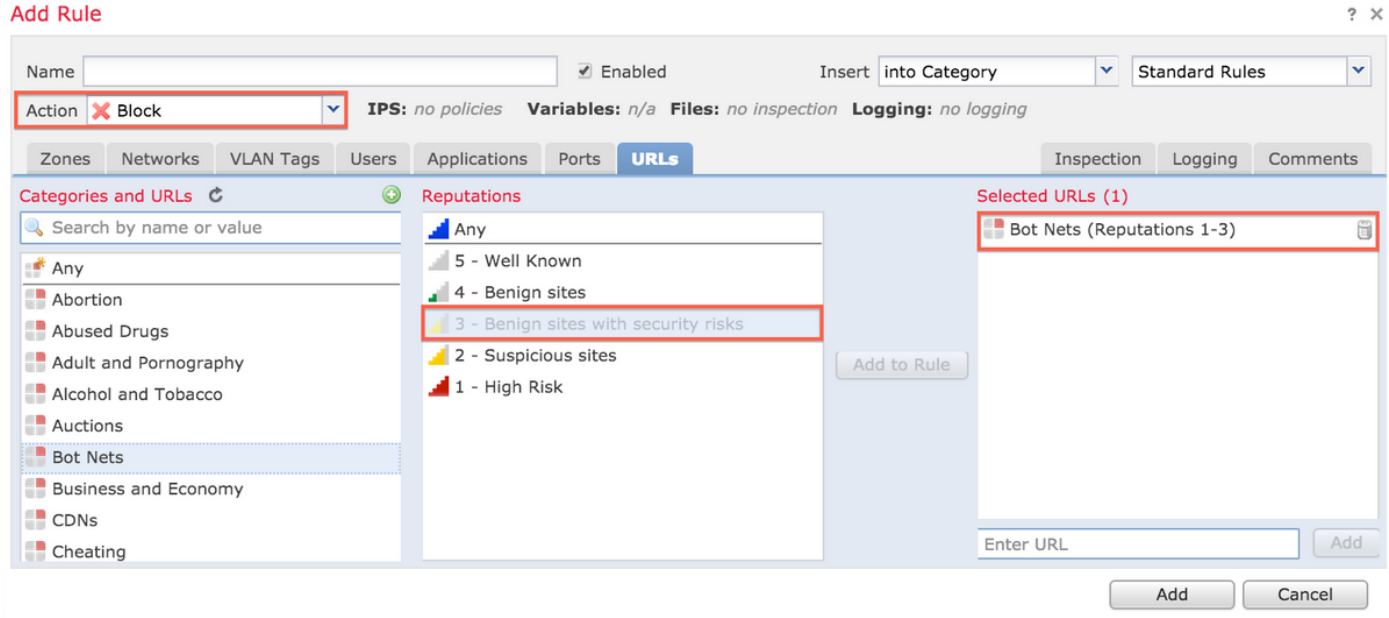
Regelaktion ist zulässig

Wenn Sie eine Regel erstellen, um Datenverkehr basierend auf einer Reputationsstufe **zuzulassen,** werden durch die Auswahl einer Reputationsstufe auch alle Reputationsstufen mit einer geringeren Sicherheit als die ursprünglich ausgewählte Stufe ausgewählt. Wenn Sie z. B. eine Regel konfigurieren, die *Gutartige Websites mit Sicherheitsrisiken* zulässt (Stufe 3), werden automatisch auch *Gutartige Websites (*Stufe 4) und *Bekannte* Websites (Stufe 5) zugelassen.



Regelaktion ist gesperrt

Wenn Sie eine Regel erstellen, um Datenverkehr auf Grundlage einer Reputationsstufe zu **blockieren,** werden durch die Auswahl einer Reputationsstufe auch alle Reputationsstufen ausgewählt, die strenger sind als die ursprünglich ausgewählte Stufe. Wenn Sie z. B. eine Regel konfigurieren, die *Gutartige Websites mit Sicherheitsrisiken (*Stufe 3) blockiert, blockiert sie automatisch auch *verdächtige Websites (*Stufe 2) und *Websites mit hohem Risiko (*Stufe 1).



URL-Auswahlmatrix

Ausgewählte Reputationsstufe	Ausgewählte Regelaktion				
	Hohes Risiko	**Verdächtige Website**	**Unbedenkliche Website mit Sicherheitsrisiko**	**Benigner Standort**	**Bekan**
1 - Hohes Risiko	Sperren, Zulassen	Zulassen	Zulassen	Zulassen	Zulas
2 - Verdächtige Websites	Blockieren	Sperren, Zulassen	Zulassen	Zulassen	Zulas
3 - Unbedenkliche Websites mit	Blockieren	Blockieren	Sperren, Zulassen	Zulassen	Zulas

Sicherheitsrisiken					
4 - Gutartige Websites	Blockieren	Blockieren	Blockieren	Sperren, Zulassen	Zulas
5 - Bekannt	Blockieren	Blockieren	Blockieren	Blockieren	Sperr Zulas

Problem 2: Platzhalter funktioniert nicht in der Zugriffskontrollregel

Das FireSIGHT-System unterstützt nicht die Angabe eines Platzhalters in einer URL-Bedingung. Diese Bedingung kann unter cisco.com zu einer Warnung führen.

```
*cisco*.com
```

Darüber hinaus kann eine unvollständige URL mit anderem Datenverkehr übereinstimmen, was zu einem unerwünschten Ergebnis führt. Wenn Sie einzelne URLs unter URL-Bedingungen angeben, müssen Sie anderen möglicherweise betroffenen Datenverkehr sorgfältig prüfen. Stellen Sie sich beispielsweise ein Szenario vor, in dem Sie cisco.com explizit blockieren möchten. Die Zuordnung von Teilzeichenfolgen bedeutet jedoch, dass die Sperrung von cisco.com auch sanfrancisco.com blockiert, was möglicherweise nicht Ihre Absicht ist.

Wenn Sie eine URL eingeben, geben Sie den Domänennamen ein, und lassen Sie die Informationen zur Unterdomäne aus. Geben Sie z. B. cisco.com statt www.cisco.com ein. Wenn Sie cisco.com in einer **Zulassungsregel** verwenden, können Benutzer zu einer der folgenden URLs navigieren:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

Problem 3: URL-Kategorie und Reputation sind nicht ausgefüllt

Wenn sich eine URL nicht in einer lokalen Datenbank befindet und sie zum ersten Mal im Datenverkehr erkannt wird, wird möglicherweise keine Kategorie oder Reputation eingetragen. Das bedeutet, dass eine unbekannte URL beim ersten Mal nicht mit der AC-Regel übereinstimmt. Manchmal werden die URL-Suchvorgänge für häufig besuchte URLs möglicherweise nicht aufgelöst, wenn eine URL zum ersten Mal erkannt wird. Dieses Problem wurde in den Versionen 5.3.0.3, 5.3.1.2 und 5.4.0.2, 5.4.1.1 behoben.

Zugehörige Informationen

- Konfiguration der URL-Filterung auf einem FireSIGHT-System
- Technischer Support und Dokumentation für Cisco Systeme