

Benutzerdefinierte URL-Kategorien in WSA definieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[URLs zulassen](#)

[Erstellen einer neuen benutzerdefinierten URL](#)

[Globale Zugriffsrichtlinie bearbeiten](#)

[URLs sperren](#)

[Erstellen einer neuen benutzerdefinierten URL](#)

[Globale Zugriffsrichtlinie bearbeiten](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie benutzerdefinierte URL-Kategorien in der Websicherheits-Appliance (WSA) definieren können.

Beitrag von Shikha Grover und Herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der Cisco Web Security Appliance für Anfänger

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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

Die Kategorie, in die eine URL fällt, wird durch eine Filterkategorien-Datenbank bestimmt. Die Web Security Appliance erfasst Informationen und verwaltet für jedes URL-Filtermodul eine separate Datenbank. Die Datenbanken der Filterkategorien erhalten regelmäßig Updates vom Cisco Update-Server und werden von Cisco TALOS verwaltet. Talos, die Security Intelligence and Research Group von Cisco, verfolgt kontinuierlich eine Vielzahl von Attributen, um Rückschlüsse auf einen bestimmten Host zu ziehen.

Es kann Situationen geben, in denen Sie eine URL/Domäne/IP-Adresse anders klassifizieren möchten und eine benutzerdefinierte Klassifizierung lokal auf Ihrem Gerät haben. Dies können Sie mit benutzerdefinierten URL-Kategorien erreichen.

Wenn das URL-Filtermodul eine URL-Kategorie mit der URL in einer Clientanforderung vergleicht, wertet es die URL zuerst mit den benutzerdefinierten URL-Kategorien aus, die in der Richtliniengruppe enthalten sind. Wenn die URL in der Anforderung nicht mit einer enthaltenen benutzerdefinierten Kategorie übereinstimmt, vergleicht das URL-Filtermodul sie mit den vordefinierten URL-Kategorien.

Konfigurieren

URLs zulassen

Wenn Sie der Website vertrauen, können Sie sie mit dem folgenden Prozess zulassen.

Erstellen einer neuen benutzerdefinierten URL

1. Erstellen Sie eine neue benutzerdefinierte URL-Kategorie, navigieren Sie zu GUI > Web Security Manager > Benutzerdefinierte URL-Kategorien > Benutzerdefinierten Kategorienamen hinzufügen: Zulässige URLs.
2. Fügen Sie die Websites hinzu, die Sie im Abschnitt "Sites" kontrollieren möchten (company.com, .company.com).

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	Allowed URLs
Comments: ?	
List Order:	1
Category Type:	Local Custom Category
Sites: ?	company.com, .company.com (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Advanced	Regular Expressions: ? Enter one regular expression per line.

- 3.
4. Bitte beachten Sie, dass "domain.com" nur mit "domain.com" übereinstimmt, nicht mit

www.domain.com oder "host.domain.com". Um eine Site und alle Unterdomänen zuzulassen, sind im Abschnitt "Sites" zwei Einträge erforderlich: ". domain.com, domain.com".

5. Klicken Sie auf Senden.

Globale Zugriffsrichtlinie bearbeiten

1. Öffnen Sie Websicherheits-Manager > Zugriffsrichtlinien > Globale Richtlinie > URL-Filterung.
2. Klicken Sie auf Benutzerdefinierte Kategorien auswählen.
3. Klicken Sie auf den Pfeil des Dropdown-Menüs Zugelassene URLs, wählen Sie In Richtlinie einschließen, und klicken Sie auf Anwenden.
4. Aktivieren Sie das Kontrollkästchen Zulassen.
5. Klicken Sie auf Senden und Änderungen bestätigen.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering	
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.	
Category	Category Type
Allowed URLs	Custom (LOCK)
Select Custom Categories	

URLs sperren

Wenn Sie der Website nicht vertrauen, können Sie sie mit dem folgenden Prozess blockieren.

Erstellen einer neuen benutzerdefinierten URL

1. Erstellen Sie eine neue benutzerdefinierte URL-Kategorie, navigieren Sie zu GUI > Web Security Manager > Benutzerdefinierte URL-Kategorien > Benutzerdefinierten Kategorienamen hinzufügen: Gesperrte URLs.
2. Fügen Sie die Websites hinzu, die Sie kontrollieren möchten, im Abschnitt "Sites" (company.com, .company.com).

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	Blocked URLs
Comments: (?)	
List Order:	1
Category Type:	Local Custom Category
Sites: (?)	company.com, .company.com Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)
Advanced	Regular Expressions: (?) Enter one regular expression per line.

[Cancel](#) [Submit](#)

- Bitte beachten Sie, dass "domain.com" nur mit "domain.com" übereinstimmt, nicht mit www.domain.com oder "host.domain.com". Um eine Site und alle untergeordneten Domänen zu blockieren, sind zwei Einträge im Abschnitt "Sites" erforderlich: ". domain.com, domain.com".
- Klicken Sie auf Senden.

Globale Zugriffsrichtlinie bearbeiten

- Öffnen Sie Websicherheits-Manager > Zugriffsrichtlinien > Globale Richtlinie > URL-Filterung.
- Klicken Sie auf Benutzerdefinierte Kategorien auswählen...
- Klicken Sie auf den Pfeil des Dropdown-Menüs Blockierte URLs, wählen Sie In Richtlinie einschließen, und klicken Sie auf Anwenden.
- Aktivieren Sie das Kontrollkästchen Block (Blockieren).
- Klicken Sie auf Senden und Änderungen bestätigen.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering								
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.								
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-based	Time-based
Blocked URLs	Custom (Local)	Select all	Select all	Select all	Select all	Select all		
Select Custom Categories...								

 Hinweis: Die oben genannten Änderungen können an jeder Zugriffsrichtlinie und nicht nur an der globalen Richtlinie vorgenommen werden. Das gleiche Verfahren kann auf Entschlüsselungsrichtlinien angewendet werden.

In diesem [Leitfaden](#) finden Sie einen weit verbreiteten Anwendungsfall.

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.