

Blockieren des Google AI-Modus in der sicheren Web-Appliance

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die erforderlichen Schritte beschrieben, um die Secure Web Appliance so zu konfigurieren, dass HTTPS-Anfragen an den Google AI-Modus blockiert werden.

Voraussetzungen

Anforderungen

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

- SWA-Verwaltung
- Grundlegende Netzwerk- und Proxy-Protokolle
- Entschlüsselungsprozess der SWA
- Reguläre Ausdrücke

Cisco empfiehlt die Installation der folgenden Tools:

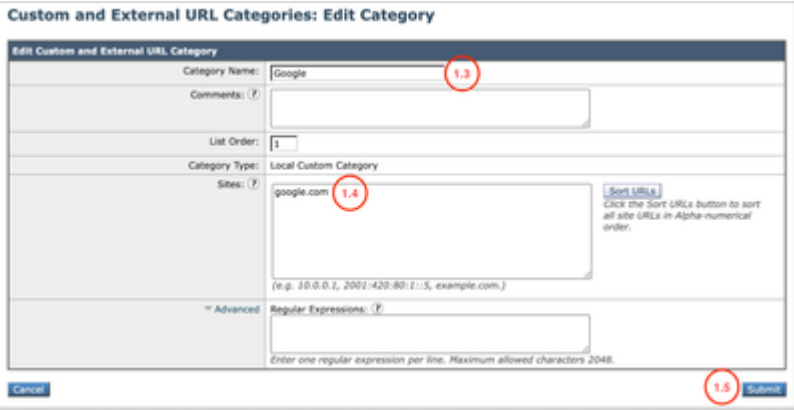
- Physisches oder virtuelles SWA
- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) von SWA

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.

Konfigurationsschritte

<p>Schritt 1: Erstellen einer benutzerdefinierten URL-Kategorie für die Google-Website</p>	<p>Schritt 1.1: Navigieren Sie in der GUI zum Websicherheits-Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus.</p> <p>Schritt 1.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen.</p> <p>Schritt 1.3. Geben Sie einen Namen für die neue Kategorie ein.</p> <p>Schritt 1.4. Definieren Sie diese URLs im Abschnitt Sites: google.com</p> <p>Schritt 1.5. Senden Sie die Änderungen.</p> 
<p>Schritt 2. Erstellen Sie eine benutzerdefinierte URL-Kategorie für den Google AI-Modus.</p>	<p>Schritt 2.1: Navigieren Sie in der GUI zum Websicherheits-Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus.</p> <p>Schritt 2.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen.</p>

Schritt 2.3: Geben Sie für die neue Kategorie einen Namen ein.

Schritt 2.4. Definieren Sie diese URLs im Abschnitt Reguläre Ausdrücke:

google\.com.*udm=50

Schritt 2.5. Senden Sie die Änderungen.



Tip: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter [Benutzerdefinierte URL-Kategorien konfigurieren in der sicheren Webappliance - Cisco](#)

Custom and External URL Categories: Edit Category

Advanced Regular Expressions: google\.com.*udm=50

Schritt 3. Entschlüsseln Sie den Datenverkehr für Google.

Schritt 3.1: Navigieren Sie in der GUI zum Websicherheits-Manager, und wählen Sie Entschlüsselungsrichtlinien aus.

Schritt 3.2. Klicken Sie auf Richtlinie hinzufügen.

Schritt 3.3: Geben Sie einen Namen für die neue Richtlinie ein.

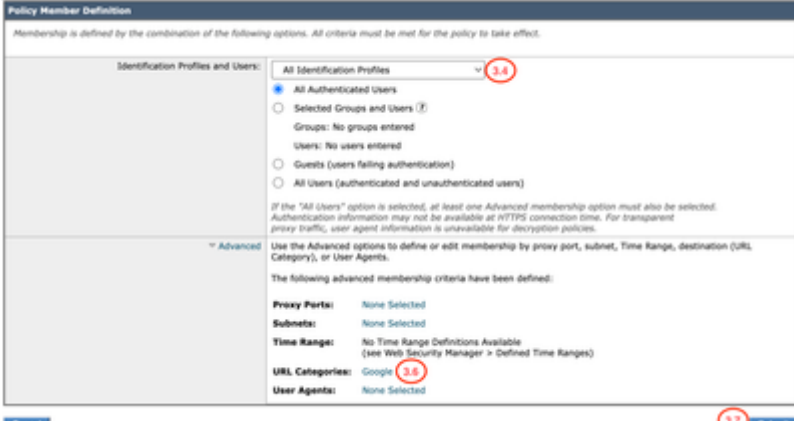
Schritt 3.4 (Optional) Wählen Sie das Identifikationsprofil

aus, auf das diese Richtlinie angewendet werden soll.

Schritt 3.5: Klicken Sie im Abschnitt Definition der Richtlinienmitglieder auf URL-Kategorien-Links, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 3.6: Wählen Sie die URL-Kategorie, die in Schritt 1 erstellt wurde.

Schritt 3.7. Klicken Sie auf Senden.



Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

- All Identification Profiles (3.5)
- All Authenticated Users
- Selected Groups and Users (0)
- Groups: No groups entered
- Users: No users entered
- Guests (users failing authentication)
- All Users (Authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

- Proxy Ports: None Selected
- Subnets: None Selected
- Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
- URL Categories: Google (3.6)
- User Agents: None Selected

Cancel Submit (3.7)

Schritt 3.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Schritt 3.9. Wählen Sie Entschlüsseln als Aktion für die benutzerdefinierte URL-Kategorie aus.

Schritt 3.10. Klicken Sie auf Senden.

Decryption Policies: URL Filtering: Decrypting Google Traffic



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	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Google	Custom (Local)	Select all	Select all	Select all	Select all (3.9)	Select all	(Unavailable)	(Unavailable)

Cancel Submit (3.10)

Schritt 4: Blockieren des Datenverkehrs im Google AI-Modus

Schritt 4.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Zugriffsrichtlinien aus.

Schritt 4.2. Klicken Sie auf Richtlinie hinzufügen.

Schritt 4.3: Geben Sie einen Namen für die neue Richtlinie ein.

Schritt 4.4 (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.

Schritt 4.5: Klicken Sie im Abschnitt Policy Member Definition (Richtlinienmitgliedsdefinition) auf die Links URL-Kategorien, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 4.6: Wählen Sie die in Schritt 2 erstellte URL-Kategorie.

Schritt 4.7. Klicken Sie auf Senden.

Schritt 4.8. Klicken Sie auf der Seite "Access Policies" (Zugriffsrichtlinien) auf den Link von URL Filtering, um die neue Richtlinie zu erhalten.

Schritt 4.9. Wählen Sie Blockieren als Aktion für die benutzerdefinierte URL-Kategorie.

Schritt 4.10. Klicken Sie auf Senden.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Rewrite Profile	Clone Policy	Delete
1	Google AI Block Identification Profile: All identified users URL Categories: GoogleModeAIblock	(global policy)	Block 1	Monitor: X11	(global policy)	(global policy)	(global policy)		

Überprüfung

Wenn die Konfigurationseinstellungen abgeschlossen sind, wird der Google AI-Datenverkehr in den Zugriffsprotokollen als Block verarbeitet, da er von der benutzerdefinierten Kategorie, die wir für den Google AI-Block erstellt haben, erkannt wird.

<#root>

1779219170.427 101 10.184.103.26

TCP_DENIED_SSL/403

0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo

BLOCK_CUSTOMCAT_12-Google_AI_Block

-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-,-,-,"IW_srch"

Eine Anfrage für eine Suchanfrage im Google AI-Modus wird blockiert und zeigt diese Endbenutzerbenachrichtigung an.



Der restliche Google-Datenverkehr ist weiterhin zulässig.

Zugehörige Informationen

[Benutzerdefinierte URL-Kategorien in WSA definieren](#)

[Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance](#)

[Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren](#)

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.