Sperren des Zugriffs auf Google-Privatkundenkonten in den SWAs

Inhalt

Einleitung

Dieses Dokument beschreibt den Prozess der Blockierung des Zugriffs auf Google Workspace oder Google Consumer Accounts in Secure Web Appliance (SWA).

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA.

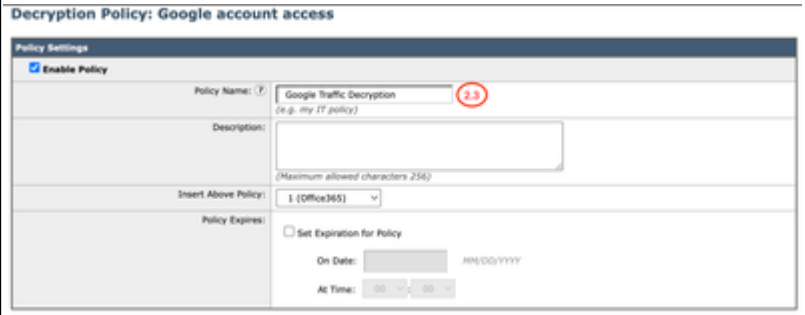
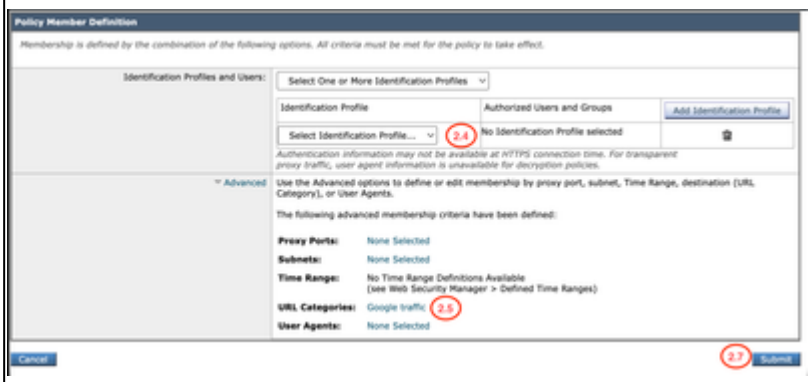
Verwendete Komponenten

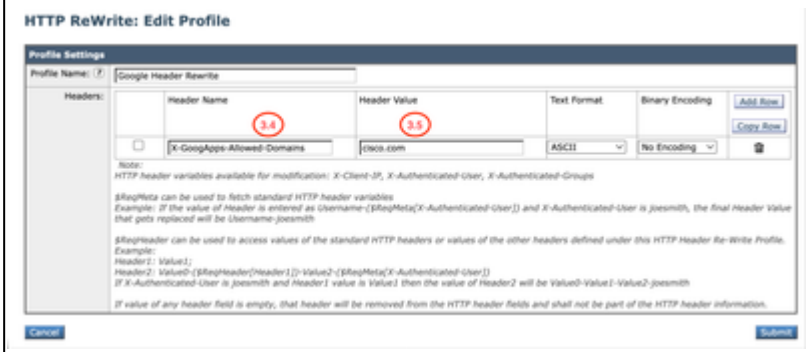
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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.

Konfigurieren

Schritt 1.Erstellen Sie eine benutzerdefinierte URL-Kategorie für die Google-Websites.	Schritt 1.1: Navigieren Sie in der GUI zum Web Security Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus. Schritt 1.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen. Schritt 1.3: Geben Sie einen Namen für die neue Kategorie ein. Schritt 1.4. Definieren Sie diese URLs im Abschnitt Sites: `.google.com` Schritt 1.5. Änderungen übermitteln.  Bild - Benutzerdefinierte URL-Kategorie Tipp: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter: Konfigurieren benutzerdefinierter URL-Kategorien in der sicheren Webappliance.

Schritt 2:Entschlüsseln des Datenverkehrs	Schritt 2.1. Navigieren Sie in der GUI zuWebsicherheits-Manager, und wählen Sie Entschlüsselungsrichtlinien aus. Schritt 2.2. Klicken Sie auf Richtlinie hinzufügen. Schritt 2.3: EnterName für die neue Richtlinie.  Schritt 2.4: Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll. Tipp: Wenn Sie die Authentifizierungen für Microsoft-URLs umgangen haben und diese Richtlinie für Alle Benutzer konfigurieren, wählen Sie: Alle Identifizierungsprofile > Alle Benutzer. Schritt 2.5. Klicken Sie im Abschnitt "Policy Member Definition" auf URL-KategorienLinks, um die benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 2.6.Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde. Schritt 2.7: Klicken Sie auf Senden.  Image: Konfigurieren der Entschlüsselungsrichtlinie Schritt 2.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung

	für die neue Richtlinie.  Bild - URL-Filterungsaktion bearbeiten Schritt 2.9. Wählen Sie Entschlüsseln als Aktion für die benutzerdefinierte URL-Kategorie aus. Schritt 2.10.Klicken Sie auf Senden.  Bild: Entschlüsseln der benutzerdefinierten URL-Kategorie
Schritt 3: Erstellen eines HTTP Rewrite Profile	Schritt 3.1.Navigieren Sie in der GUI zuWeb Security Manager und wählen Sie HTTP ReWrite Profiles. Schritt 3.2. Klicken Sie auf Profil hinzufügen. Schritt 3.3: Geben Sie einen Namen für das neue Profil ein. Schritt 3.4: Verwenden Sie X-GoogApps-Allowed-Domains als ersten Header-Namen. Schritt 3.5. Für die Einstellung "Restrict-Access-To-Tenants" verwenden Sie einen Domänenwert der Liste zulässiger Tenants, bei der es sich um eine kommagetrennte Liste der Tenants handeln muss, auf die Benutzer zugreifen dürfen. Schritt 3.9.Klicken Sie auf Senden.  Bild - HTTP ReWrite-Profil hinzufügen

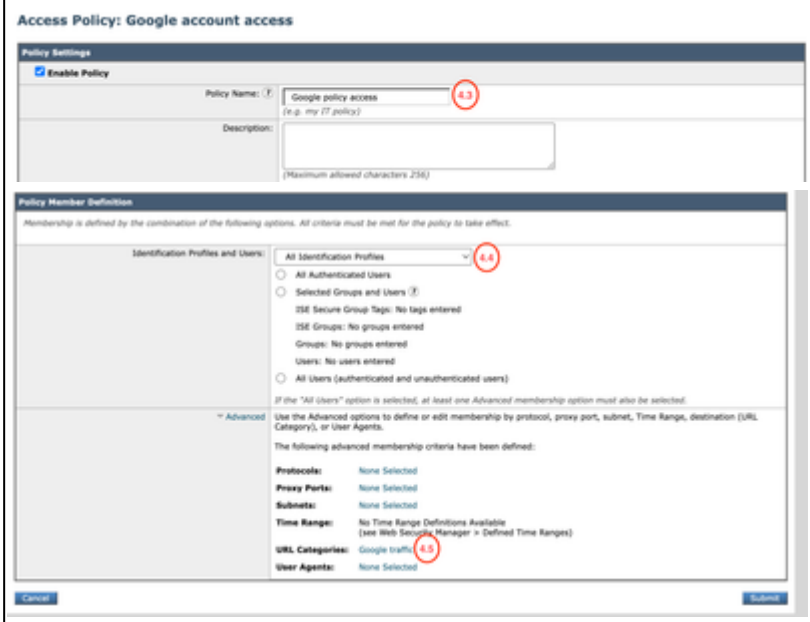
Schritt 4:Erstellen einer Zugriffsrichtlinie	Schritt 4.1. Navigieren Sie in der GUI zuWebsicherheits-Manager, und wählen Sie Zugriffsrichtlinien aus. Schritt 4.2. Klicken Sie auf Richtlinie hinzufügen. Schritt 4.3: EnterName für die neue Richtlinie. Schritt 4.4 (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll. Schritt 4.5.Klicken Sie im Abschnitt "Policy Member Definition" auf URL-KategorienLinks, um die benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 4.6.Wählen Sie die in Schritt 1 erstellte URL-Kategorie aus. Schritt 4.7. Klicken Sie auf Senden.  Bild: Erstellen einer Zugriffsrichtlinie Schritt 4.8.Stellen Sie auf der Seite Access Policies (Zugriffsrichtlinien) sicher, dass die Aktion der URL-Filterung auf Monitor (Überwachen) festgelegt ist. Schritt 4.9:Klicken Sie auf den Link in HTTP ReWrite Profile, um dieser Richtlinie das HTTP-Header-Profil hinzuzufügen.

Bild - Eigenschaften der Zugriffsrichtlinie

Schritt 4.10: Wählen Sie die HTTP-ReWrite-Profile, die in Schritt [3] erstellt wurden.

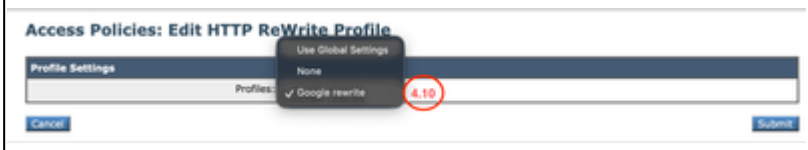


Bild - HTTP ReWrite-Profil hinzufügen

Schritt 4.11. Klicken Sie aufSenden.

Schritt 4.12. Änderungen bestätigen.

Berichte und Protokolle

Protokolle

Sie können den Zugriffsprotokollen oder den W3C-Protokollen benutzerdefinierte Felder hinzufügen, um den Namen des HTTP-Header-Umschreibprofils anzuzeigen.

Formatangabe in Zugriffsprotokollen	Protokollfeld in W3C-Protokollen	Beschreibung
%]	x-http-rewrite-profilname	Profilname für HTTP-Header umschreiben.

Sie können einen Web-Tracking-Bericht erstellen, um die Berichte des Datenverkehrs nach dem Namen der Zugriffsrichtlinie anzuzeigen.

Gehen Sie folgendermaßen vor, um Berichte zu erstellen:

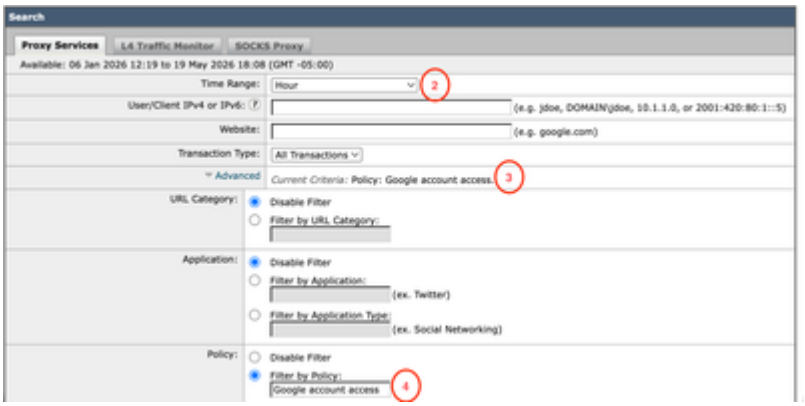
Schritt 1: Wählen Sie in der GUI Reporting aus, und wählen Sie Web Tracking aus.

Schritt 2: Wählen Sie den gewünschten Zeitraum.

Schritt 3: Klicken Sie auf den Link Erweitert, um Transaktionen nach erweiterten Kriterien zu suchen.

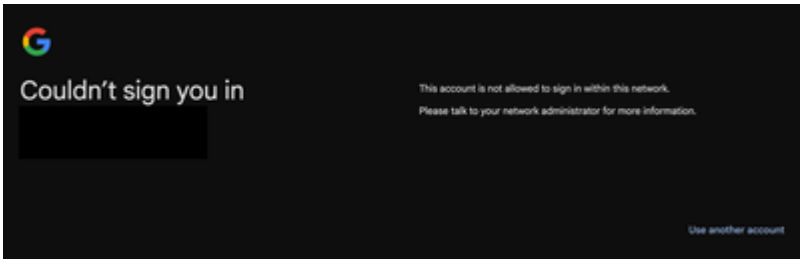
Schritt 4. Wählen Sie im Abschnitt Policy (Richtlinie) die Option Filter by Policy (Nach Richtlinie filtern) aus, und geben Sie den Namen der zuvor erstellten Zugriffsrichtlinie ein.

Schritt 5: Klicken Sie auf Suchen, um den Bericht zu überprüfen.



Überprüfung

Wenn die Konfiguration der Google-Domänenbeschränkung abgeschlossen ist, kann der Benutzer nur auf die Konten zugreifen, die sich unter der im Header Rewrite-Profil in Schritt 3 konfigurierten Domäne befinden. Wenn die Benutzer versuchen, auf ein Konto in einer anderen Domäne oder, in einem anderen, persönlichen Google-Konto zuzugreifen, wird der Zugriff mit diesem Hinweis eingeschränkt:



Zugehörige Informationen

Benutzerdefinierte URL-Kategorien in WSA definieren

Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance

Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren

WSA HTTP Header Rewrite

Zugriff auf Verbraucherkonten blockieren (Google-Dokumentation)

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.