Upload-Verkehr in sicherer Web-Appliance blockieren

Inhalt

Einleitung

In diesem Dokument wird der Prozess zum Blockieren des Upload-Verkehrs zu bestimmten Websites in der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

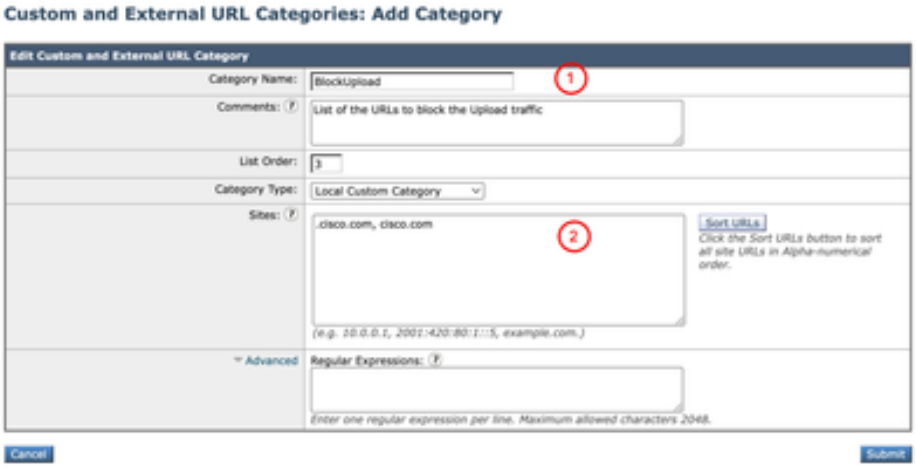
Verwendete Komponenten

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.

Konfigurationsschritte

Schritt 1: Erstellen einer	Schritt 1.1. Navigieren Sie in der GUI zu Web Security Manager,

benutzerdefinierten URL-Kategorie für die Website	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 den Namen für die neue Kategorie ein. Schritt 1.4. Definieren Sie die Domäne und/oder Subdomänen der Website, die Sie versuchen, den Upload-Datenverkehr zu blockieren (in diesem Beispiel cisco.com und alle Subdomänen). Schritt 1.5.Senden Sie die Änderungen.  Bild: Benutzerdefinierte URL-Kategorie erstellen Tipp: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Schritt 2: Entschlüsseln des Datenverkehrs für die URL	Schritt 2.1. Navigieren Sie in der GUI zum Web Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus. Schritt 2.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 2.3: Geben Sie den Namen für die neue Richtlinie ein. Schritt 2.4. (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll. Schritt 2.5. Klicken Sie im Abschnitt Definition der Richtlinienmitglieder auf URL-Kategorien-Links, 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.

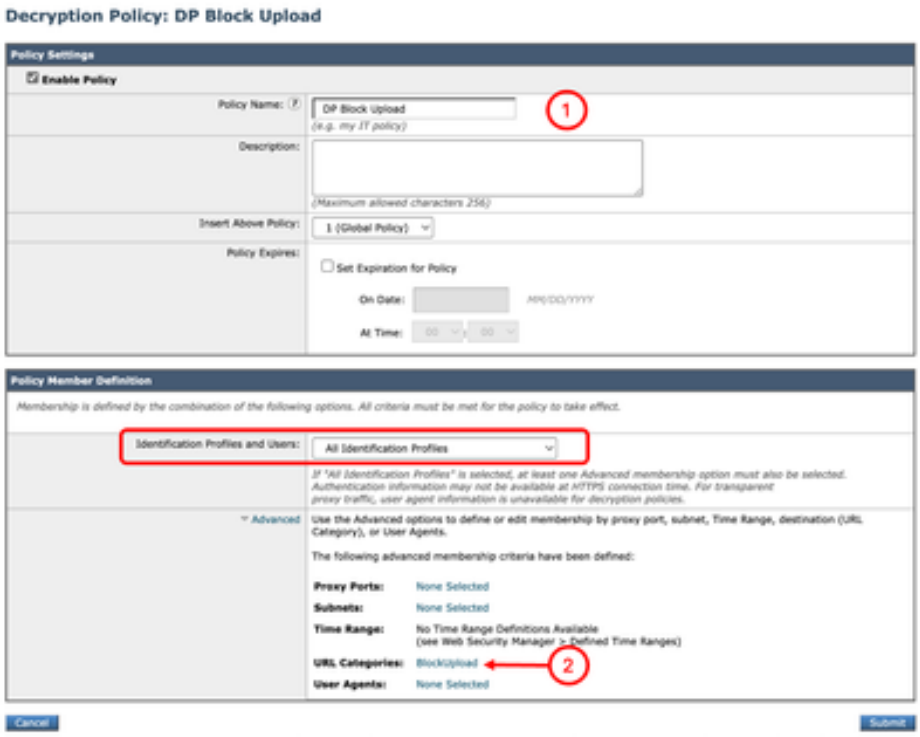


Bild - Entschlüsselungsrichtlinie erstellen

Schritt 2.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Bild: Auswahl der URL-Filterung

Schritt 2.9. Wählen Sie Entschlüsseln als Aktion für die benutzerdefinierte URL-Kategorie aus.

Schritt 2.10. Klicken Sie auf Senden.

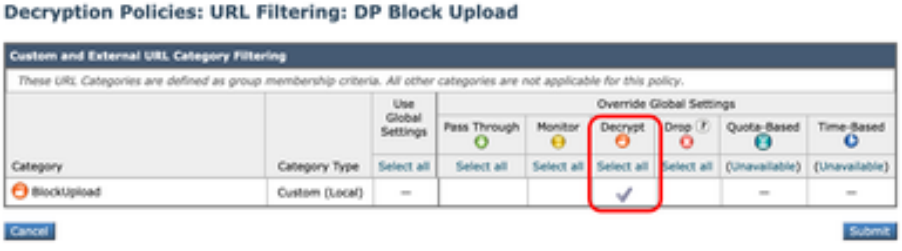


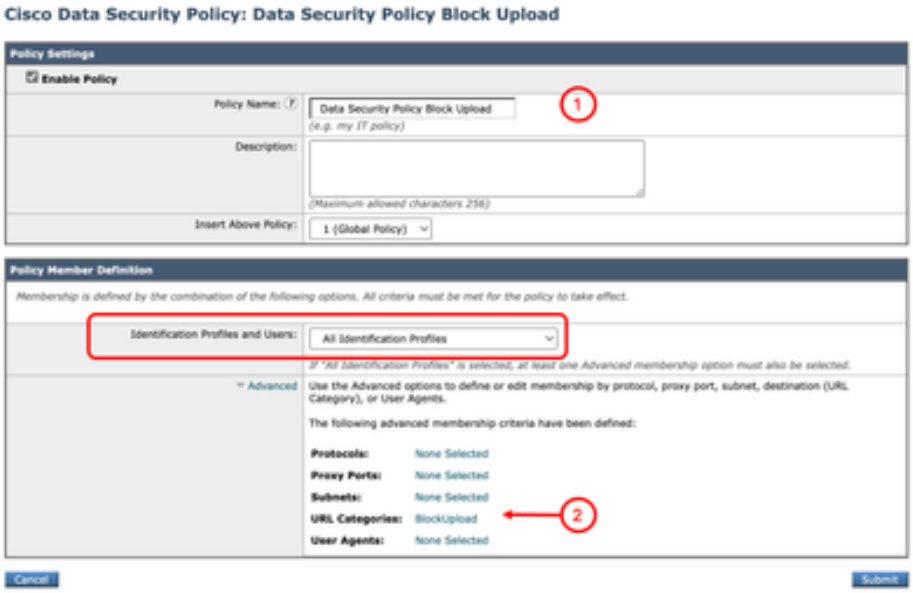
	Bild - Als Aktion entschlüsseln
Schritt 3: Blockieren des Upload-Datenverkehrs	Schritt 3.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Cisco Data Security aus. Schritt 3.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 3.3: Geben Sie den Namen für die neue Richtlinie ein. Schritt 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 die Links URL-Kategorien, um die benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 3.6. Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde. Schritt 3.7: Klicken Sie auf Senden.  Bild: Cisco Datensicherheitsrichtlinie Tipp: Für die Berichterstellung empfiehlt es sich, einen Namen zu wählen, der nicht mit anderen Zugriffs-/Entschlüsselungsrichtlinien übereinstimmt. Schritt 3.8: Klicken Sie auf der Seite Cisco Date Security Policy (Cisco Richtlinie für Datumssicherheit) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Bild: Auswahl der URL-Filterung

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

Schritt 3.10. Klicken Sie auf Senden.

Bild - Hochladen blockieren

Schritt 3.11: Änderungen bestätigen.

Berichte und Protokolle

Protokolle

Sie können die Protokolle für den Upload-Datenverkehr über die CLI anzeigen, indem Sie dissdataloss_logs auswählen, der Standardprotokollierungsname für Datensicherheitsprotokolle.

Gehen Sie folgendermaßen vor, um auf die Protokolle zuzugreifen:

Schritt 1: Anmeldung bei der CLI

Schritt 2. Geben Sie grep ein, und drücken Sie die Eingabetaste.

Schritt 3. Suchen und geben Sie die Nummer ein, die mit idsdataloss_logs verknüpft ist:

- Typ: "Data Security Logs"
- Abruf: FTP Poll und drücken die Eingabetaste.

Schritt 4. (Optional) Geben Sie den regulären Ausdruck ein, um Sie nach Schlüsselwörtern zu filtern, oder drücken Sie die Eingabetaste, um alle Protokolle anzuzeigen.

Schritt 5. (Optional) Soll bei dieser Suche die Groß-/Kleinschreibung beachtet werden? [Y]> Wenn Sie in Schritt 4 Schlüsselwörter auswählen, können Sie den Filter unabhängig von der Groß-/Kleinschreibung auswählen.

6. Schritt (Optional) Möchten Sie nach nicht übereinstimmenden Posten suchen? [N]> Falls Sie alle Protokolle mit Ausnahme der in Schritt 4 definierten Schlüsselwörter filtern müssen, können Sie diesen Abschnitt verwenden. Andernfalls drücken Sie die Eingabetaste.

Schritt 7. (Optional) Möchten Sie die Protokolle zurückverfolgen? [N]> Wenn Sie die Live-Protokolle anzeigen möchten, geben Sie Y ein, und drücken Sie die Eingabetaste. Drücken Sie andernfalls die Eingabetaste, um alle verfügbaren Protokolle anzuzeigen.

Schritt 8. (Optional) Möchten Sie die Ausgabe paginieren? [N]> Wenn die Ergebnisse pro Seite angezeigt werden sollen, können Sie Y eingeben und die Eingabetaste drücken. Andernfalls drücken Sie die Eingabetaste, um den Standardwert zu verwenden [N].

Berichterstellung

Sie können einen Web Tracking-Bericht erstellen, um die Berichte über den blockierten Upload-Datenverkehr nach dem Richtliniennamen Cisco Data Security anzuzeigen.

Gehen Sie folgendermaßen vor, um Berichte zu erstellen:

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

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 Cisco Data Security ein, die zuvor erstellt wurde.

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

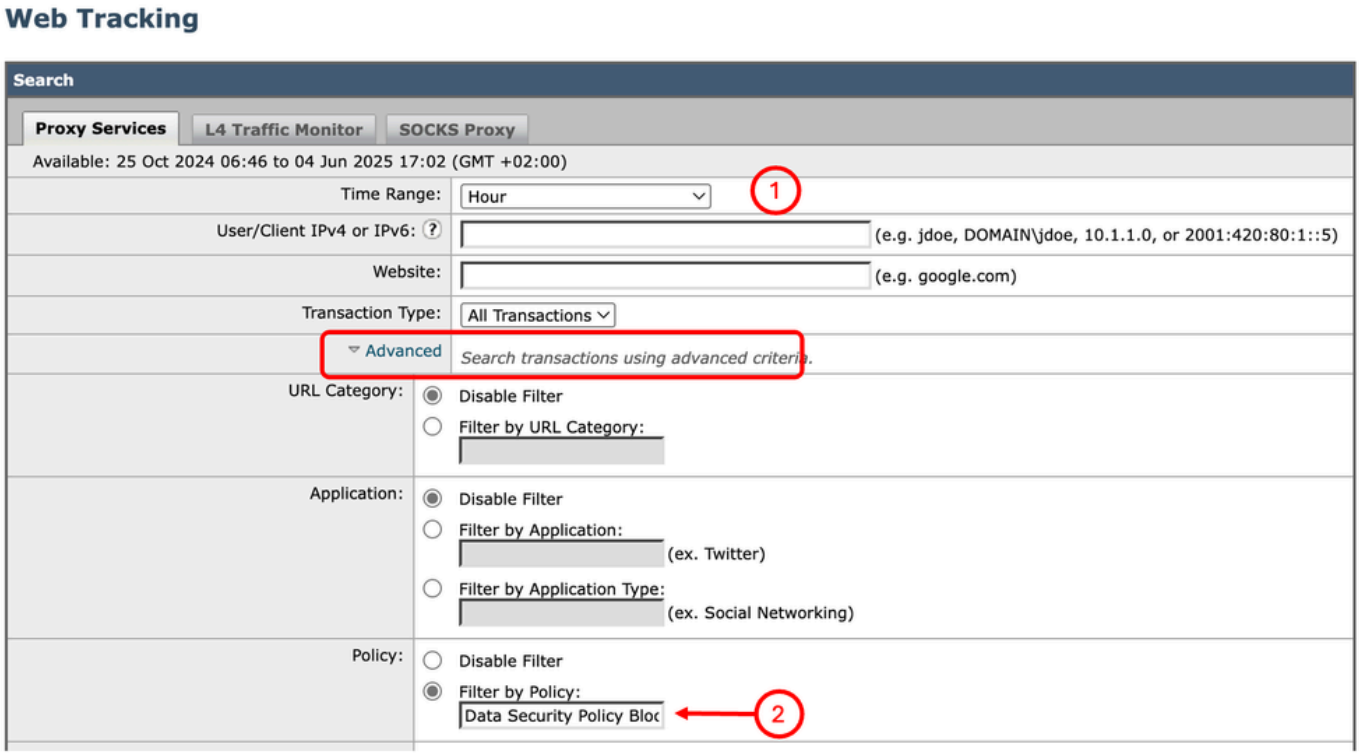


Bild - Filtern der Web-Tracking-Berichte

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Best Practices für sichere Web-Appliances
- Firewall für sichere Web-Appliance konfigurieren
- Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren
- SNMP in SWA konfigurieren und Fehlerbehebung dafür durchführen
- Konfigurieren von SCP-Push-Protokollen in der sicheren Web-Appliance mit Microsoft Server
- Aktivierung bestimmter YouTube-Kanäle/Videos und Blockierung sonstiger YouTube-Inhalte in SWA
- HTTPS-Zugriffsformat in sicherer Web-Appliance
- Zugreifen auf Protokolle der sicheren Web-Appliance
- Umgehen der Authentifizierung in einer sicheren Web-Appliance
- Blockieren von Datenverkehr in einer sicheren Web-Appliance

- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance

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.