

# Konfigurieren benutzerdefinierter URL-Kategorien in der sicheren Webappliance

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Benutzerdefinierte URL-Kategorien](#)

[URL-Kategorien für Live-Feeds](#)

[Schritte zum Erstellen von benutzerdefinierten URL-Kategorien](#)

[Reguläre Ausdrücke verwenden](#)

[Einschränkungen und Design-Aspekte](#)

[Benutzerdefinierte URL-Kategorien in Richtlinien verwenden](#)

[Schritte zum Konfigurieren von URL-Filtern für die Zugriffsrichtlinie](#)

[Schritte zum Konfigurieren von URL-Filtern für die Entschlüsselungsrichtlinie](#)

[Schritte zum Konfigurieren von URL-Filtern für Datensicherheitsrichtliniengruppen](#)

[Schritte zum Konfigurieren der Steuerung von Upload-Anforderungen mit benutzerdefinierten URL-Kategorien](#)

[Schritte zum Konfigurieren von ControlUpload-Anforderungen in Richtlinien für externen SvD](#)

[Umgehungs- und Passthrough-URLs](#)

[Webproxy-Umgehung für Webanforderungen konfigurieren](#)

[Berichte](#)

[Benutzerdefinierte URL-Kategorien im Zugriffsprotokoll anzeigen](#)

[Fehlerbehebung](#)

[Kategorie nicht zugeordnet](#)

[Referenz](#)

---

## Einleitung

In diesem Dokument wird die Struktur der URL-Kategorien (Custom Uniform Resource Locator) in Secure Web Appliance (SWA) beschrieben.

## Voraussetzungen

### Anforderungen

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

- Wie Proxy funktioniert.
- Verwaltung der Secure Web Appliance (SWA).

Cisco empfiehlt Folgendes:

- Physische oder Virtual Secure Web Appliance (SWA) installiert.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.
  
- 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.


## Benutzerdefinierte URL-Kategorien

Das URL-Filter-Modul ermöglicht das Filtern von Transaktionen in Zugriffs-, Entschlüsselungs- und Datensicherheitsrichtlinien. Wenn Sie URL-Kategorien für Richtliniengruppen konfigurieren, können Sie Aktionen für benutzerdefinierte URL-Kategorien (sofern definiert) und vordefinierte URL-Kategorien konfigurieren.

Sie können benutzerdefinierte und externe Live-Feed-URL-Kategorien erstellen, die bestimmte Hostnamen und IP-Adressen beschreiben. Außerdem können Sie URL-Kategorien bearbeiten und löschen.

Wenn Sie diese benutzerdefinierten URL-Kategorien in derselben Access, Decryption oder Cisco Data Security Policy-Gruppe einschließen und jeder Kategorie unterschiedliche Aktionen zuweisen, hat die Aktion der höher eingeschlossenen benutzerdefinierten URL-Kategorie Vorrang.

---

 Hinweis: Wenn Domain Name System (DNS) mehrere IPs in eine Website auflöst und eine dieser IPs eine benutzerdefinierte Sperrliste ist, blockiert die Websicherheits-Appliance die Website für alle IPs, unabhängig davon, ob sie nicht in der benutzerdefinierten Sperrliste aufgeführt sind.

---

## URL-Kategorien für Live-Feeds

Externe Live-Feed-Kategorien werden verwendet, um die Liste der URLs von einer bestimmten Website abzurufen, z. B. zum Abrufen der Office 365-URLs von Microsoft.

Wenn Sie beim Erstellen und Bearbeiten von benutzerdefinierten und externen URL-Kategorien für den Kategorietyt Externe Live-Feed-Kategorie auswählen, müssen Sie das Feed-Format (Cisco Feed-Format oder Office 365 Feed-Format) auswählen und dann eine URL für den entsprechenden Feed-Datei-Server angeben.

Das erwartete Format für die einzelnen Feed-Dateien sieht wie folgt aus:

- Cisco Feed-Format - Dies muss eine CSV-Datei (Comma-Separated Values, durch Komma getrennte Werte) sein, d. h. eine Textdatei mit der Erweiterung .csv. Jeder Eintrag in der CSV-Datei muss in einer separaten Zeile im Format Adresse/Komma/Adresstyp stehen. (z. B.: [www.cisco.com/site](http://www.cisco.com/site) oder ad2.\*\com,regex). Gültige Adresstypen sind site und regex.

Hier ein Auszug aus einer CSV-Datei im Cisco Feed-Format:

```
www.cisco.com,site
\.xyz,regex
ad2.*\com,regex
www.cisco.local,site
1:1:1:1:1:1::200,site
```


- Office 365-Feed-Format - Dies ist eine XML-Datei auf einem Microsoft Office 365-Server oder einem lokalen Server, auf dem Sie die Datei gespeichert haben. Es wird vom Office 365-Dienst bereitgestellt und kann nicht geändert werden.

Die Netzwerkadressen in der Datei sind in XML-Tags eingeschlossen. Diese Struktur lautet: Produkte > Produkt > Adressliste > Adresse. In der aktuellen Implementierung kann ein "Adresslistentyp" IPv6, IPv4 oder URL sein [dieser kann Domänen und reguläre Ausdrücke (Regex) enthalten].

Hier ist ein Ausschnitt einer Office 365-Feed-Datei:

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
</products>
```

---

 Hinweis: Schließen Sie `http://` oder `https://` nicht als Teil eines Websiteeintrags in die Datei ein, da andernfalls ein Fehler auftritt. Mit anderen Worten: [www.cisco.com](http://www.cisco.com) wird korrekt geparkt, während <http://www.cisco.com> einen Fehler erzeugt

---

## Schritte zum Erstellen benutzerdefinierter URL-Kategorien

Schritt 1: Wählen Sie Websicherheits-Manager > Benutzerdefinierte und externe URL-Kategorien.

## **Authentication**

Identification Profiles

SaaS Policies

## **Web Policies**

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

## **Data Transfer Policies**

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies


## **Custom Policy Elements**

Custom and External URL Categories

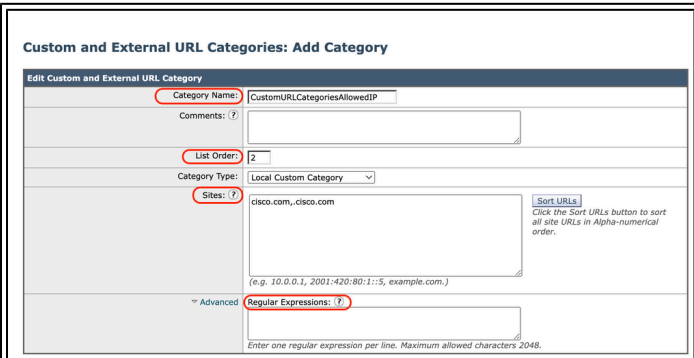
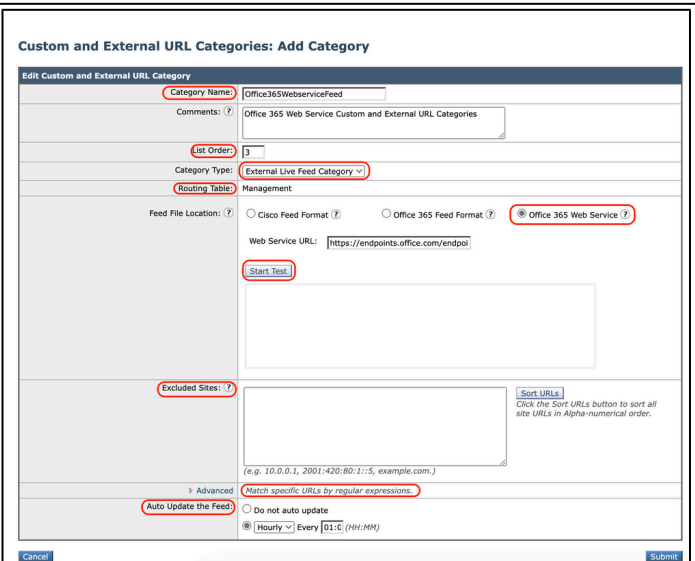
Geben Sie einen Bezeichner für diese URL-Kategorie ein. Dieser Name wird angezeigt, wenn Sie den URL-Filter für Richtliniengruppen konfigurieren.

- Listenreihenfolge: Geben Sie die Reihenfolge dieser Kategorie in der Liste der benutzerdefinierten URL-Kategorien an. Geben Sie "1" für die erste URL-Kategorie in der Liste ein.

Das URL-Filtermodul wertet eine Clientanforderung anhand der benutzerdefinierten URL-Kategorien in der angegebenen Reihenfolge aus.

 Hinweis: Wenn das URL-Filtermodul eine URL-Kategorie mit der URL in einer Clientanforderung vergleicht, vergleicht es die URL zuerst mit den benutzerdefinierten URL-Kategorien in der Richtliniengruppe. Wenn die URL in der Anforderung nicht mit einer enthaltenen benutzerdefinierten Kategorie übereinstimmt, vergleicht das URL-Filtermodul sie mit den vordefinierten URL-Kategorien. Wenn die URL keiner der enthaltenen benutzerdefinierten oder vordefinierten URL-Kategorien entspricht, wird die Anforderung nicht kategorisiert.

- Kategorietyt: Wählen Sie Lokale benutzerdefinierte Kategorie oder externe Live-Feed-Kategorie aus.
- Routingtabelle: Wählen Sie Management oder Data (Daten). Diese Option ist nur verfügbar, wenn "Split-Routing" aktiviert ist, d. h. nicht für lokale benutzerdefinierte Kategorien verfügbar.

 <p>image-Lokale benutzerdefinierte URL-Kategorie</p>	 <p>Image: Feeds für benutzerdefinierte URL-Kategorie konfigurieren</p>
Lokale benutzerdefinierte Kategorie	Externe Live-Feed-Kategorie

## Reguläre Ausdrücke verwenden

Die Secure Web Appliance verwendet eine Syntax für reguläre Ausdrücke, die sich geringfügig von der Syntax für reguläre Ausdrücke unterscheidet, die von anderen Implementierungen der Velocity Pattern-Matching-Engine verwendet wird.

Außerdem unterstützt die Appliance keinen umgekehrten Schrägstrich, um einen umgekehrten Schrägstrich zu vermeiden. Wenn Sie einen Schrägstrich in einem regulären Ausdruck verwenden möchten, geben Sie einfach den Schrägstrich ohne umgekehrten Schrägstrich ein.


---

 Hinweis: Technisch verwendet AsyncOS für Web den Flex-Analyzer für reguläre Ausdrücke


---

Um Ihre regulären Ausdrücke zu testen, können Sie diesen Link benutzen: [flex lint - Regex Tester/Debugger](#)

---

 Achtung: Reguläre Ausdrücke, die mehr als 63 Zeichen zurückgeben, schlagen fehl und erzeugen einen Fehler bei ungültigen Einträgen. Stellen Sie sicher, dass Sie reguläre Ausdrücke erstellen, die nicht mehr als 63 Zeichen zurückgeben können.

---

 Vorsicht: Reguläre Ausdrücke, die umfangreiche Zeichen ausführen, nehmen Ressourcen auf und können die Systemleistung beeinträchtigen. Aus diesem Grund können reguläre Ausdrücke vorsichtig angewendet werden.

---

Sie können reguläre Ausdrücke an folgenden Stellen verwenden:

- Benutzerdefinierte URL-Kategorien für Zugriffsrichtlinien Wenn Sie eine benutzerdefinierte URL-Kategorie für Zugriffsrichtlinien-Gruppen erstellen, können Sie mit regulären Ausdrücken mehrere Webserver angeben, die dem von Ihnen eingegebenen Muster entsprechen.
  - Benutzerdefinierte Benutzer-Agents blockieren. Wenn Sie die zu blockierenden Anwendungen für eine Zugriffsrichtliniengruppe bearbeiten, können Sie mithilfe regulärer Ausdrücke bestimmte Benutzer-Agents für die Blockierung eingeben.
- 


 Tipp: Sie können die Umgehung des Webproxys für reguläre Ausdrücke nicht festlegen.

---

Hier ist die Liste der Zeichenklassen in regulärem Flex-Ausdruck

Zeichenklassen	
.	Alle Zeichen außer Zeilenumbruch
\w \d \s	Wort, Ziffer, Leerzeichen
\W \D \S	kein Wort, keine Ziffer, Leerzeichen
[Abc]	a, b oder c
[^abc]	nicht a, b oder c
[a-g]	Zeichen zwischen a & g
Anker	
^abc\$	Anfang / Ende der Zeichenkette
\b	Wortgrenze
Escapezeichen	
\* \\	Sonderzeichen mit Escapezeichen

<code>\t \n \r</code>	Tab, Zeilenvorschub, Wagenrücklauf
<code>\u00A9</code>	Unicode entwichen ©
Gruppen und Lookaround	
<code>(abc)</code>	Fanggruppe
<code>\1</code>	zurück zur Gruppe #1
<code>(?:abc)</code>	nicht erfassende Gruppe
<code>(?=abc)</code>	positiver Ausblick
<code>(?!abc)</code>	negativer Ausblick
Quantifizierer und Alternativen	
<code>a* a+ a?</code>	0 oder mehr, 1 oder mehr, 0 oder 1
<code>a{5} a{2},</code>	genau fünf, zwei oder mehr
<code>a{1,3}</code>	zwischen einem und drei
<code>a+? a{2,}?</code>	so wenig wie möglich übereinstimmen
<code>ab cd</code>	Übereinstimmung ab oder cd

 **Vorsicht:** Seien Sie vorsichtig bei unentwegten Punkten in langen Mustern, und besonders in der Mitte längerer Muster, und seien Sie vorsichtig bei diesem Metazeichen (Stern \*), besonders in Verbindung mit dem Punktzeichen. Jedes Muster enthält einen Punkt ohne Escapezeichen, der mehr als 63 Zeichen zurückgibt, nachdem der Punkt deaktiviert wurde. Immer entkommen \*(Stern) und . (Punkt) mit \ ( umgekehrter Schrägstrich ) wie \`*` und \`.` Wenn wir `.cisco.local` im regulären Ausdruck verwenden, stimmt auch die Domain `Xcisco.local` überein.

Der unverwischte Charakter beeinflusst die Leistung und es erzeugt Langsamkeit während des Web-Browsing. Dies liegt daran, dass die Pattern-Matching-Engine Tausende oder Millionen von Möglichkeiten durchlaufen muss, bis sie eine Übereinstimmung für den richtigen Eintrag findet. Außerdem kann sie Sicherheitsbedenken hinsichtlich ähnlicher URLs für zulässige Richtlinien haben.

Sie können die Befehlszeilenschnittstellenoption (CLI) `advanced proxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex, to enable or disable default regex convertierung to lower case for case-insensitive matching`. Verwenden Sie dieses Kontrollkästchen, wenn bei der Groß-/Kleinschreibung Probleme auftreten.

## Einschränkungen und Design-Aspekte

- Sie können in diesen URL-Kategoriedefinitionen nicht mehr als 30 externe Live-Feed-Dateien verwenden, und jede Datei darf nicht mehr als 5000 Einträge enthalten.
- Wenn die Anzahl der externen Einspeisungen zunimmt, führt dies zu Leistungseinbußen.
- Es ist möglich, dieselbe Adresse in mehreren benutzerdefinierten URL-Kategorien zu verwenden, aber die Reihenfolge, in der die Kategorien aufgeführt werden, ist relevant.

Wenn Sie diese Kategorien in derselben Richtlinie einschließen und für jede Kategorie



unterschiedliche Aktionen definieren, wird die Aktion angewendet, die für die in der Tabelle der benutzerdefinierten URL-Kategorien am höchsten aufgeführte Kategorie definiert ist.

- Wenn eine native FTP-Anforderung (File Transfer Protocol) transparent an den FTP-Proxy umgeleitet wird, enthält sie keine Hostnamen-Informationen für den FTP-Server, sondern nur dessen IP-Adresse.

Aus diesem Grund stimmen einige vordefinierte URL-Kategorien und Webreputations-Filter, die nur über Hostnamen-Informationen verfügen, nicht mit nativen FTP-Anforderungen überein, selbst wenn die Anforderungen für diese Server bestimmt sind.

Wenn Sie den Zugriff auf diese Websites blockieren möchten, müssen Sie benutzerdefinierte URL-Kategorien erstellen, damit diese ihre IP-Adressen verwenden können.

- Eine nicht kategorisierte URL ist eine URL, die keiner vordefinierten URL-Kategorie oder integrierten benutzerdefinierten URL-Kategorie entspricht.

## Benutzerdefinierte URL-Kategorien in Richtlinien verwenden

Das URL-Filter-Modul ermöglicht das Filtern von Transaktionen in Zugriffs-, Entschlüsselungs- und Datensicherheitsrichtlinien. Wenn Sie URL-Kategorien für Richtliniengruppen konfigurieren, können Sie Aktionen für benutzerdefinierte URL-Kategorien (sofern definiert) und vordefinierte URL-Kategorien konfigurieren.

### Schritte zum Konfigurieren von URL-Filtern für die Zugriffsrichtlinie

Schritt 1: Wählen Sie Websicherheits-Manager > Zugriffsrichtlinien aus.

## Authentication

Identification Profiles

SaaS Policies

## Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

## Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

## Custom Policy Elements

Klicken Sie in der Richtlinientabelle in der Spalte URL-Filter für die Richtliniengruppe, die Sie bearbeiten möchten, auf den Link.

### Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	<b>Access Policy</b> Identification Profile: Global All identified users	(global policy)	(global policy)	Monitor: 343	(global policy)	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 107	Monitor: 343	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Bild: Benutzerdefinierte Kategorie zur Zugriffsrichtlinie hinzufügen

Schritt 3. (Optional) Im Abschnitt Benutzerdefinierte URL-Kategoriefilterung können Sie benutzerdefinierte URL-Kategorien hinzufügen, für die in dieser Richtlinie Maßnahmen ergriffen werden sollen:

a) Klicken Sie auf Benutzerdefinierte Kategorien auswählen.

### Access Policies: URL Filtering: Access Policy

**Custom and External URL Category Filtering**

*No Custom Categories are included for this Policy.*

[Select Custom Categories...](#)

Benutzerdefinierte URL-Kategorie für Bildauswahl

b) Wählen Sie die benutzerdefinierten URL-Kategorien aus, die in dieser Richtlinie enthalten sein sollen, und klicken Sie auf Apply.

**Select Custom Categories for this Policy** ✕

Category	Category Type	Setting Selection
Msoffice365Feed	External Feed	Exclude from policy <span style="float: right;">▼</span>
CustomURLCategoriesA...	Custom (Local)	Include in policy <span style="float: right;">▼</span>
Office365WebserviceF...	External Feed	Use Global Settings (Exclude from policy) <span style="float: right;">▼</span>

[Cancel](#)
[Apply](#)

Image - Wählen Sie benutzerdefinierte Kategorien aus, die in die Richtlinie eingeschlossen werden sollen.

Wählen Sie aus, mit welchen benutzerdefinierten URL-Kategorien das URL-Filtermodul die

Clientanforderung vergleichen muss.

Das URL-Filtermodul vergleicht Clientanforderungen mit enthaltenen benutzerdefinierten URL-Kategorien und ignoriert ausgeschlossene benutzerdefinierte URL-Kategorien.

Das URL-Filtermodul vergleicht die URL in einer Clientanforderung mit integrierten benutzerdefinierten URL-Kategorien vor vordefinierten URL-Kategorien.

Die benutzerdefinierten URL-Kategorien, die in der Richtlinie enthalten sind, werden im Abschnitt zur Filterung nach benutzerdefinierten URL-Kategorien angezeigt.

Schritt 4: Wählen Sie im Abschnitt zur Filterung benutzerdefinierter URL-Kategorien eine Aktion für jede enthaltene benutzerdefinierte URL-Kategorie aus.

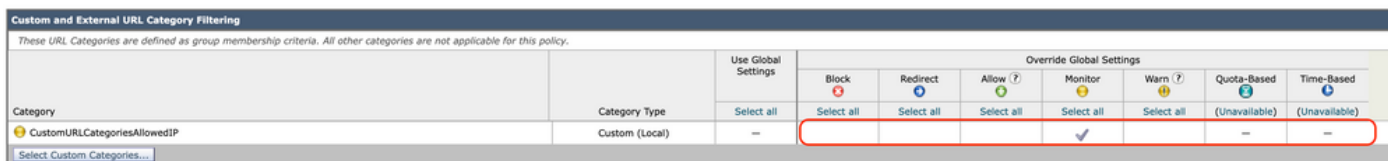


Bild - Aktion für benutzerdefinierte Kategorie auswählen

Aktion	Beschreibung
Globale Einstellungen verwenden	Verwendet die Aktion für diese Kategorie in der globalen Richtliniengruppe. Dies ist die Standardaktion für benutzerdefinierte Richtliniengruppen. Nur für benutzerdefinierte Richtliniengruppen.
Blockieren	Der Webproxy verweigert Transaktionen, die mit dieser Einstellung übereinstimmen.
Umleiten	Lenkt Datenverkehr, der ursprünglich für eine URL in dieser Kategorie bestimmt war, an einen von Ihnen angegebenen Speicherort um. Wenn Sie diese Aktion auswählen, wird das Feld Umleiten an angezeigt. Geben Sie eine URL ein, an die der gesamte Datenverkehr umgeleitet werden soll.
Zulassen	Ermöglicht immer Clientanforderungen für Websites in dieser Kategorie. Zulässige Anfragen umgehen alle weiteren Filter und Malware-Scans. Verwenden Sie diese Einstellung nur für vertrauenswürdige Websites. Sie können diese Einstellung für interne Sites verwenden.
Überwachung	Der Webproxy lässt die Anforderung weder zu noch blockiert er sie.

Aktion	Beschreibung
	Stattdessen wird die Client-Anforderung anhand anderer Einstellungen zur Richtliniengruppen-Kontrolle, z. B. des Web-Reputationsfilters, ausgewertet.
Warnen	Der Webproxy blockiert zunächst die Anforderung und zeigt eine Warnseite an. Der Benutzer kann jedoch fortfahren, indem er auf einen Hypertext-Link auf der Warnseite klickt.
kontingentbasiert	Wenn sich ein einzelner Benutzer dem von Ihnen angegebenen Volumen- oder Zeitkontingent nähert, wird eine Warnung angezeigt. Wenn ein Kontingent erreicht wurde, wird eine Blockseite angezeigt. .
Zeitbasiert	Der Webproxy blockiert oder überwacht die Anforderung während der von Ihnen angegebenen Zeiträume.

Schritt 5: Wählen Sie im Abschnitt Vordefinierter URL-Kategoriefilter eine der folgenden Aktionen für jede Kategorie aus:

- Globale Einstellungen verwenden
- Überwachung
- Warnen
- Blockieren
- Zeitbasiert
- kontingentbasiert

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn (?)	Quota-Based	Time-Based
Animals and Pets	Select all	Select all	Select all	Select all		
Arts			Select all			
Redefined Quota Profile: 10GBdailyLimit Astrology In time range: MorningShift Action: Warn Otherwise: Block						

Bild - Aktion für vordefinierte Kategorie auswählen

Schritt 6: Wählen Sie im Abschnitt Nicht kategorisierte URLs die Aktion aus, die für Clientanforderungen an Websites ausgeführt werden soll, die nicht in eine vordefinierte oder benutzerdefinierte URL-Kategorie fallen. Diese Einstellung legt auch die Standardaktion für neue

und zusammengeführte Kategorien fest, die sich aus Aktualisierungen des URL-Kategoriesatzes ergeben.

Uncategorized URLs	
<i>Specify an action for urls that do not match any category.</i>	
Uncategorized URLs:	Monitor
Default Action for Update Categories: ?	Most Restrictive

Bild: Aktion für nicht kategorisierte URL auswählen

Schritt 7. Senden und bestätigen Sie Änderungen.

Schritte zum Konfigurieren von URL-Filtern für die Entschlüsselungsrichtlinie

Schritt 1: Wählen Sie Websicherheits-Manager > Entschlüsselungsrichtlinien aus.

## **Authentication**

Identification Profiles

SaaS Policies

## **Web Policies**

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

## **Data Transfer Policies**

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

## **Custom Policy Elements**

Klicken Sie in der Richtlinientabelle in der Spalte URL-Filterung auf den Link für die Richtliniengruppe, die Sie bearbeiten möchten.

### Decryption Policies

Policies						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	<b>DecryptionPolicy</b> Identification Profile: Global All identified users	(global policy)	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	Monitor: 1 Decrypt: 106 Drop: 1	Enabled	Decrypt		

Bild: URL-Filter auswählen

Schritt 3. (Optional) Im Abschnitt Benutzerdefinierte URL-Kategoriefilterung können Sie benutzerdefinierte URL-Kategorien hinzufügen, für die in dieser Richtlinie Maßnahmen ergriffen werden sollen:

- a. Klicken Sie auf Benutzerdefinierte Kategorien auswählen.

### Decryption Policies: URL Filtering: DecryptionPolicy

Custom and External URL Category Filtering
No Custom Categories are included for this Policy.
Select Custom Categories...

Bild - Benutzerdefinierte Kategorien auswählen

- b. Wählen Sie die benutzerdefinierten URL-Kategorien, die in dieser Richtlinie enthalten sein sollen, und klicken Sie auf Apply.

Select Custom Categories for this Policy		
Category	Category Type	Setting Selection
MSOffice365Feed	External Feed	Exclude from policy
CustomURLCategoriesA...	Custom (Local)	Include in policy
Office365WebserviceF...	External Feed	Use Global Settings (Exclude from policy)

Cancel Apply

Image - Wählen Sie benutzerdefinierte Kategorien aus, die in die Richtlinie eingeschlossen werden sollen.

Wählen Sie aus, mit welchen benutzerdefinierten URL-Kategorien das URL-Filtermodul die Clientanforderung vergleichen muss.



Das URL-Filtermodul vergleicht Clientanforderungen mit enthaltenen benutzerdefinierten URL-Kategorien und ignoriert ausgeschlossene benutzerdefinierte URL-Kategorien.

Das URL-Filtermodul vergleicht die URL in einer Clientanforderung mit integrierten benutzerdefinierten URL-Kategorien vor vordefinierten URL-Kategorien.

Die benutzerdefinierten URL-Kategorien, die in der Richtlinie enthalten sind, werden im Abschnitt zur Filterung nach benutzerdefinierten URL-Kategorien angezeigt.

Schritt 4: Wählen Sie eine Aktion für jede benutzerdefinierte und vordefinierte URL-Kategorie aus.

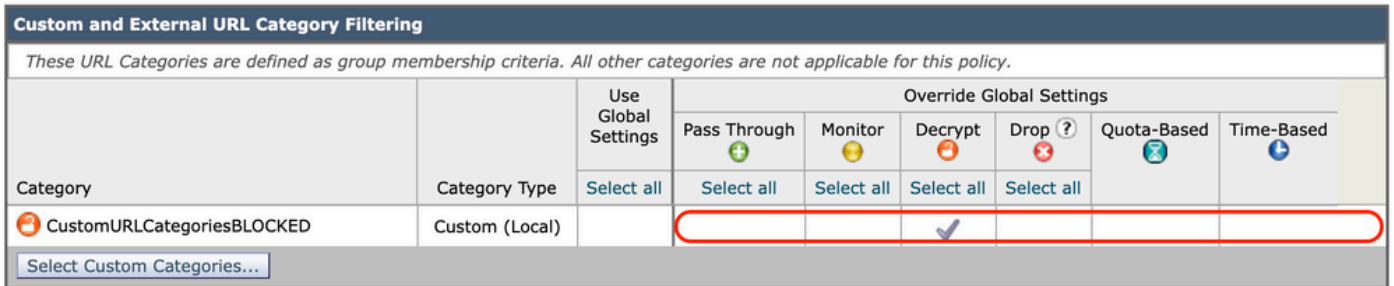


Bild - Aktion für Entschlüsselungsrichtlinie auswählen

Aktion	Beschreibung
Globale Einstellung verwenden	<p>Verwendet die Aktion für diese Kategorie in der globalen Gruppe Entschlüsselungsrichtlinie. Dies ist die Standardaktion für benutzerdefinierte Richtliniengruppen.</p> <p>Nur für benutzerdefinierte Richtliniengruppen.</p> <p>Wenn eine benutzerdefinierte URL-Kategorie in der globalen Entschlüsselungsrichtlinie ausgeschlossen wird, lautet die Standardaktion für enthaltene benutzerdefinierte URL-Kategorien in benutzerdefinierten Entschlüsselungsrichtlinien Überwachen statt Globale Einstellungen verwenden. Sie können nicht die Option Globale Einstellungen verwenden auswählen, wenn eine benutzerdefinierte URL-Kategorie in der globalen Entschlüsselungsrichtlinie ausgeschlossen wird.</p>
Pass-Through	Durchläuft die Verbindung zwischen dem Client und dem Server, ohne den Inhalt des Datenverkehrs zu überprüfen.
Überwachung	Der Webproxy lässt die Anforderung weder zu noch blockiert er sie. Stattdessen wird die Client-Anforderung anhand anderer Einstellungen zur Richtliniengruppen-Kontrolle, z. B. des Web-Reputationsfilters, ausgewertet.

Aktion	Beschreibung
Entschlüsseln	Ermöglicht die Verbindung, überprüft jedoch den Datenverkehrsinhalt. Die Appliance entschlüsselt den Datenverkehr und wendet Zugriffsrichtlinien auf den entschlüsselten Datenverkehr an, als ob es sich um eine HTTP-Verbindung (Hypertext Transfer Protocol) handeln würde. Wenn die Verbindung entschlüsselt und Zugriffsrichtlinien angewendet werden, können Sie den Datenverkehr nach Malware durchsuchen.
Verwerfen	Löscht die Verbindung und leitet die Verbindungsanforderung nicht an den Server weiter. Die Appliance benachrichtigt den Benutzer nicht, dass die Verbindung getrennt wurde.

Schritt 5: Wählen Sie im Abschnitt Nicht kategorisierte URLs die Aktion aus, die für Clientanforderungen an Websites ausgeführt werden soll, die nicht in eine vordefinierte oder benutzerdefinierte URL-Kategorie fallen.

Diese Einstellung legt auch die Standardaktion für neue und zusammengeführte Kategorien fest, die sich aus Aktualisierungen des URL-Kategoriesatzes ergeben.

Bild - Nicht kategorisierte Entschlüsselungsrichtlinie

Schritt 6: Senden und bestätigen Sie Änderungen.

**⚠** Vorsicht: Wenn Sie eine bestimmte URL-Kategorie für HTTPS-Anforderungen (Hypertext Transfer Protocol Secure) blockieren möchten, entschlüsseln Sie diese URL-Kategorie in der Gruppe Entschlüsselungsrichtlinie, und blockieren Sie dann dieselbe URL-Kategorie in der Gruppe Zugriffsrichtlinie.

## Schritte zum Konfigurieren von URL-Filtern für Datensicherheitsrichtliniengruppen

Schritt 1: Wählen Sie Web Security Manager > Cisco Data Security aus.

## **Authentication**

Identification Profiles

SaaS Policies

## **Web Policies**

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

## **Data Transfer Policies**

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

## **Custom Policy Elements**

Custom and External URL Categories

Klicken Sie in der Richtlinientabelle in der Spalte URL-Filterung auf den Link für die Richtliniengruppe, die Sie bearbeiten möchten.

## Cisco Data Security

Cisco Data Security Policies						
Add Policy...						
Order	Cisco Data Security Policy	URL Filtering	Web Reputation	Content	Clone Policy	Delete
1	<b>CiscoDataSecurityPolicy</b> Identification Profile: Global All identified users	(global policy)	(global policy)	(global policy)		
	<b>Global Policy</b> Identification Profile: All	Monitor: 107	Enabled	No maximum size for HTTP/HTTPS No maximum size for FTP		
Edit Policy Order...						

Bild - Datensicherheit URL-Filter auswählen

Schritt 3. (Optional) Im Abschnitt Benutzerdefinierte URL-Kategoriefilterung können Sie benutzerdefinierte URL-Kategorien hinzufügen, für die in dieser Richtlinie Maßnahmen ergriffen werden sollen:

- a. Klicken Sie auf Benutzerdefinierte Kategorien auswählen.

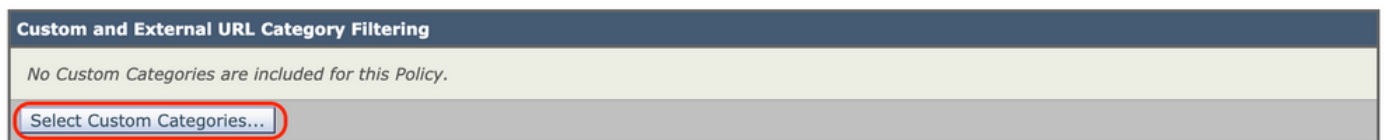


Bild - Benutzerdefiniertes Feld auswählen

- b. Wählen Sie die benutzerdefinierten URL-Kategorien, die in dieser Richtlinie enthalten sein sollen, und klicken Sie auf Apply.

### Select Custom Categories for this Policy ✕

Category	Category Type	Setting Selection
Msoffice365Feed	External Feed	Exclude from policy <span style="float: right;">▼</span>
CustomURLCategoriesA...	Custom (Local)	Include in policy <span style="float: right;">▼</span>
Office365WebserviceF...	External Feed	Use Global Settings (Exclude from policy) <span style="float: right;">▼</span>

Cancel
Apply

Image - Wählen Sie benutzerdefinierte Kategorien aus, die in die Richtlinie eingeschlossen werden sollen.

Wählen Sie aus, mit welchen benutzerdefinierten URL-Kategorien das URL-Filtermodul die Clientanforderung vergleichen muss.

Das URL-Filtermodul vergleicht Clientanforderungen mit enthaltenen benutzerdefinierten URL-

Kategorien und ignoriert ausgeschlossene benutzerdefinierte URL-Kategorien.

Das URL-Filtermodul vergleicht die URL in einer Clientanforderung mit integrierten benutzerdefinierten URL-Kategorien vor vordefinierten URL-Kategorien.

Die benutzerdefinierten URL-Kategorien, die in der Richtlinie enthalten sind, werden im Abschnitt zur Filterung nach benutzerdefinierten URL-Kategorien angezeigt.

Schritt 4: Wählen Sie im Abschnitt Benutzerdefinierte URL-Kategoriefilterung eine Aktion für jede benutzerdefinierte URL-Kategorie aus.

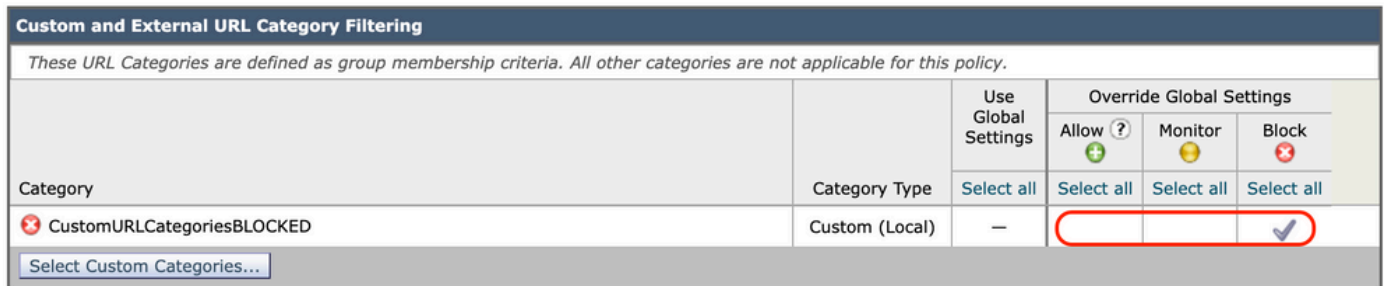


Bild: Datensicherheit - Aktion auswählen

Aktion	Beschreibung
Globale Einstellung verwenden	<p>Verwendet die Aktion für diese Kategorie in der globalen Richtliniengruppe. Dies ist die Standardaktion für benutzerdefinierte Richtliniengruppen.</p> <p>Nur für benutzerdefinierte Richtliniengruppen.</p> <p>Wenn eine benutzerdefinierte URL-Kategorie in der globalen Cisco Datensicherheitsrichtlinie ausgeschlossen wird, lautet die Standardaktion für enthaltene benutzerdefinierte URL-Kategorien in benutzerdefinierten Cisco Datensicherheitsrichtlinien Überwachen statt Globale Einstellungen verwenden. Sie können nicht die Option Globale Einstellungen verwenden auswählen, wenn eine benutzerdefinierte URL-Kategorie in der globalen Cisco Datensicherheitsrichtlinie ausgeschlossen wird.</p>
Zulassen	<p>Ermöglicht Upload-Anforderungen für Websites in dieser Kategorie immer. Nur für benutzerdefinierte URL-Kategorien.</p> <p>Zulässige Anfragen umgehen alle weiteren Datensicherheits-Scans und die Anfrage wird mit den Zugriffsrichtlinien abgeglichen.</p> <p>Verwenden Sie diese Einstellung nur für vertrauenswürdige Websites. Sie können diese Einstellung für interne Sites verwenden.</p>

Aktion	Beschreibung
Überwachung	Der Webproxy lässt die Anforderung weder zu noch blockiert er sie. Stattdessen wird die Upload-Anforderung anhand anderer Einstellungen für die Richtliniengruppen-Kontrolle ausgewertet, z. B. anhand des Web-Reputationsfilters.
Blockieren	Der Webproxy verweigert Transaktionen, die mit dieser Einstellung übereinstimmen.

Schritt 5: Wählen Sie im Abschnitt Filterung vordefinierter URL-Kategorien eine der folgenden Aktionen für jede Kategorie aus:

- Globale Einstellungen verwenden
- Überwachung
- Blockieren

Predefined URL Category Filtering			
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>			
<i>Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.</i>			
Category	Use Global Settings	Override Global Settings	
		Monitor	Block
	Select all	Select all	Select all
Hunting		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Illegal Activities		<input type="checkbox"/>	<input checked="" type="checkbox"/>

Bild - Vordefinierte URL-Aktion für Datensicherheit


Schritt 6: Wählen Sie im Abschnitt Nicht kategorisierte URLs die Aktion aus, die für Upload-Anforderungen an Websites ausgeführt werden soll, die nicht in eine vordefinierte oder benutzerdefinierte URL-Kategorie fallen.

Diese Einstellung legt auch die Standardaktion für neue und zusammengeführte Kategorien fest, die sich aus Aktualisierungen des URL-Kategoriesatzes ergeben.

Uncategorized URLs	
<i>Specify an action for urls that do not match any category.</i>	
Uncategorized URLs:	<input type="text" value="Block"/>
Default Action for Update Categories: ?	<input type="text" value="Least Restrictive"/>

Bild - Datensicherheit ohne Kategorisierung

Schritt 7. Senden und bestätigen Sie Änderungen.

 **Achtung:** Wenn Sie die Beschränkung der maximalen Dateigröße nicht deaktivieren, überprüft die Websicherheits-Appliance weiterhin die maximale Dateigröße, wenn die Optionen Zulassen oder Überwachen in der URL-Filterung ausgewählt sind.

## Schritte zum Konfigurieren der Steuerung von Upload-Anforderungen mit benutzerdefinierten URL-Kategorien

Jede Upload-Anforderung wird einer Richtliniengruppe "Scannen auf ausgehende Malware" zugewiesen und übernimmt die Kontrolleinstellungen dieser Richtliniengruppe.

Nachdem der Webproxy die Uploadanforderungs-Header empfangen hat, verfügt er über die erforderlichen Informationen, um zu entscheiden, ob er den Anforderungstext scannen muss.

Das DVS-Modul scannt die Anforderung und sendet ein Urteil an den Webproxy. Die Blockseite wird dem Endbenutzer angezeigt, falls zutreffend.

Schritt 1	Wählen Sie Web Security Manager > Scanning von ausgehender Malware aus.								
Schritt 2	Klicken Sie in der Spalte Destinations (Ziele) auf den Link für die Richtliniengruppe, die Sie konfigurieren möchten.								
Schritt 3	Wählen Sie im Abschnitt "Zieleinstellungen bearbeiten" im Dropdown-Menü die Option "Benutzerdefinierte Zielscaneinstellungen definieren" aus.								
Schritt 4	Wählen Sie im Abschnitt Zu scannende Ziele eine der folgenden Optionen aus:								
	<table border="1"><thead><tr><th>Option</th><th>Beschreibung</th></tr></thead><tbody><tr><td>Uploads nicht scannen</td><td>Das DVS-Modul scannt keine Upload-Anforderungen. Alle Upload-Anforderungen werden anhand der Zugriffsrichtlinien ausgewertet.</td></tr><tr><td>Alle Uploads scannen</td><td>Die DVS-Engine überprüft alle Upload-Anforderungen. Die Uploadanforderung wird blockiert oder anhand der Zugriffsrichtlinien ausgewertet. Dies hängt vom Scan-Verdict der DVS-Engine ab.</td></tr><tr><td>Uploads auf angegebene benutzerdefinierte URL-</td><td>Das DVS-Modul scannt Upload-Anforderungen, die zu bestimmten benutzerdefinierten URL-Kategorien</td></tr></tbody></table>	Option	Beschreibung	Uploads nicht scannen	Das DVS-Modul scannt keine Upload-Anforderungen. Alle Upload-Anforderungen werden anhand der Zugriffsrichtlinien ausgewertet.	Alle Uploads scannen	Die DVS-Engine überprüft alle Upload-Anforderungen. Die Uploadanforderung wird blockiert oder anhand der Zugriffsrichtlinien ausgewertet. Dies hängt vom Scan-Verdict der DVS-Engine ab.	Uploads auf angegebene benutzerdefinierte URL-	Das DVS-Modul scannt Upload-Anforderungen, die zu bestimmten benutzerdefinierten URL-Kategorien
	Option	Beschreibung							
	Uploads nicht scannen	Das DVS-Modul scannt keine Upload-Anforderungen. Alle Upload-Anforderungen werden anhand der Zugriffsrichtlinien ausgewertet.							
Alle Uploads scannen	Die DVS-Engine überprüft alle Upload-Anforderungen. Die Uploadanforderung wird blockiert oder anhand der Zugriffsrichtlinien ausgewertet. Dies hängt vom Scan-Verdict der DVS-Engine ab.								
Uploads auf angegebene benutzerdefinierte URL-	Das DVS-Modul scannt Upload-Anforderungen, die zu bestimmten benutzerdefinierten URL-Kategorien								

	Option	Beschreibung
	Kategorien scannen	<p>gehören. Die Upload-Anforderung wird anhand der Zugriffsrichtlinien blockiert oder ausgewertet. Dies hängt vom Scan-Urteil der DVS-Engine ab.</p> <p>Klicken Sie auf Liste der benutzerdefinierten Kategorien bearbeiten, um die zu scannenden URL-Kategorien auszuwählen.</p>
Schritt 5	Senden Sie Ihre Änderungen.	
Schritt 6	Klicken Sie in der Spalte Anti-Malware Filtering (Anti-Malware-Filterung) auf den Link der Richtliniengruppe.	
Schritt 7	Wählen Sie im Abschnitt Anti-Malware Settings (Anti-Malware-Einstellungen) die Option Define Anti-Malware Custom Settings (Benutzerdefinierte Anti-Malware-Einstellungen definieren) aus.	
Schritt 8	Wählen Sie im Abschnitt Cisco DVS Anti-Malware Settings (Cisco DVS Anti-Malware-Einstellungen) aus, welche Anti-Malware-Scan Engines für diese Richtliniengruppe aktiviert werden sollen.	
Schritt 9	<p>Wählen Sie im Abschnitt Malware-Kategorien aus, ob die verschiedenen Malware-Kategorien überwacht oder blockiert werden sollen.</p> <p>Die in diesem Abschnitt aufgelisteten Kategorien hängen davon ab, welche Scan Engines Sie aktivieren.</p>	
Schritt 10	Senden und bestätigen Sie Änderungen.	

## Schritte zum Konfigurieren von Steuerungs-Upload-Anforderungen in Richtlinien für externen SvD

Sobald der Webproxy die Upload-Anforderungsheader empfängt, verfügt er über die erforderlichen Informationen, um zu entscheiden, ob die Anforderung zum Scannen an das externe SvD-System gesendet werden kann.

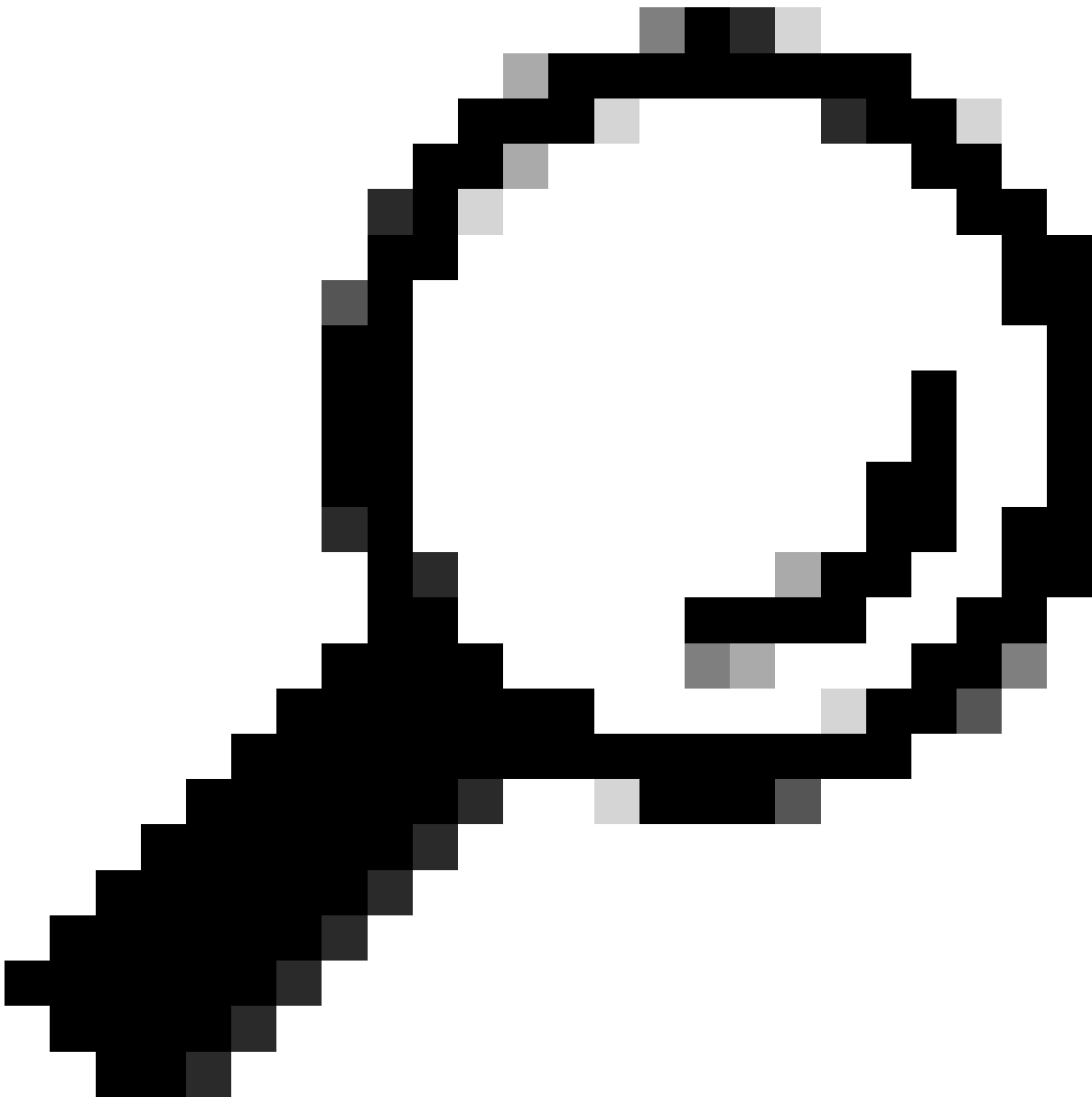


Das SvD-System scannt die Anforderung und sendet ein Urteil an den Webproxy zurück. Entweder wird die Anforderung blockiert oder überwacht (die Anforderung wird anhand der Zugriffsrichtlinien ausgewertet).

Schritt 1	Wählen Sie Web Security Manager > External Data Loss Prevention aus.
Schritt 2	Klicken Sie für die Richtliniengruppe, die Sie konfigurieren möchten, auf den Link in der Spalte "Ziele".
Schritt 3	Wählen Sie im Abschnitt "Zieleinstellungen bearbeiten" die Option "Benutzerdefinierte Zielscaneinstellungen definieren" aus.
Schritt 4	Wählen Sie im Abschnitt Ziel für Scan eine der folgenden Optionen aus: <ul style="list-style-type: none"><li>• Scannen Sie keine Uploads. An das/die konfigurierte(n) System(e) zum Schutz vor Datenverlust werden keine Upload-Anforderungen für die Suche gesendet. Alle Upload-Anforderungen werden anhand der Zugriffsrichtlinien ausgewertet.</li><li>• Alle Uploads scannen. Alle Upload-Anforderungen werden zur Überprüfung an die konfigurierten SvD-Systeme gesendet. Die Uploadanforderung wird blockiert oder anhand der Zugriffsrichtlinien ausgewertet. Dies hängt vom Ergebnis der SvD-Systemüberprüfungen ab.</li><li>• Uploads außer auf angegebene benutzerdefinierte und externe URL-Kategorien scannen. Upload-Anforderungen, die in bestimmte benutzerdefinierte URL-Kategorien fallen, werden von SvD-Scanrichtlinien ausgeschlossen. Klicken Sie auf Liste der benutzerdefinierten Kategorien bearbeiten, um die zu scannenden URL-Kategorien auszuwählen.</li></ul>
Schritt 5	Senden und bestätigen Sie Änderungen.


## URLs umgehen und weiterleiten

Sie können die Secure Web Appliance in einer transparenten Proxy-Implementierung so konfigurieren, dass HTTP- oder HTTPS-Anforderungen von bestimmten Clients oder an bestimmte Ziele umgangen werden.



Tipp: Sie können Passthrough für Anwendungen verwenden, die Datenverkehr benötigen, um die Appliance zu passieren, ohne dass Änderungen oder Zertifikatprüfungen der Zielsever erforderlich sind.

---

 Achtung: Die Domänenzuordnungsfunktion funktioniert im transparenten HTTPS-Modus. Diese Funktion funktioniert nicht im Explicit-Modus und für HTTP-Datenverkehr.

---

- Lokale benutzerdefinierte Kategorie muss konfiguriert werden, damit der Datenverkehr diese Funktion nutzen kann.
- Wenn diese Funktion aktiviert ist, kann der Servername entsprechend dem in der Domänenzuordnung konfigurierten Servernamen geändert oder zugewiesen werden, selbst wenn SNI-Informationen (Server Name Indication) verfügbar sind.

- Diese Funktion blockiert keinen Datenverkehr basierend auf dem Domänennamen, wenn dieser Datenverkehr mit der Domänenzuordnung übereinstimmt und eine benutzerdefinierte Kategorie, Entschlüsselungsrichtlinie und Passthrough-Aktion konfiguriert wurden.
- Die Authentifizierung funktioniert mit dieser Durchleitungsfunktion nicht. Die Authentifizierung erfordert eine Entschlüsselung, in diesem Fall wird der Datenverkehr jedoch nicht entschlüsselt.
- wird nicht überwacht. Sie müssen den UDP-Datenverkehr so konfigurieren, dass er nicht an die Websicherheits-Appliance übermittelt wird, sondern direkt über die Firewall in das Internet für Anwendungen wie WhatsApp, Telegram usw. geleitet wird.
- WhatsApp, Telegram und Skype funktionieren im transparenten Modus. Einige Apps wie WhatsApp funktionieren jedoch aufgrund von Einschränkungen für die App nicht im expliziten Modus.

Stellen Sie sicher, dass Sie über eine Identifizierungsrichtlinie für die Geräte verfügen, die Datenverkehr an bestimmte Server weiterleiten müssen. Im Einzelnen müssen Sie:

- Wählen Sie Von Authentifizierung/Identifikation ausnehmen.
- Geben Sie die Adressen an, auf die dieses Identifikationsprofil angewendet werden soll. Sie können IP-Adressen, CIDR-Blöcke (Classless Inter-Domain Routing) und Subnetze verwenden.

Schritt 1	HTTPS-Proxy aktivieren.
Schritt 2	<p>Wählen Sie Web Security Manager &gt; Domain Map aus.</p> <ul style="list-style-type: none"> <li>a. Wählen Sie Domäne hinzufügen aus.</li> <li>b. Geben Sie den Domänennamen oder den Zielservers ein.</li> <li>c. Wählen Sie die Reihenfolge der Priorität aus, wenn einige Domänen angegeben sind.</li> <li>d. Geben Sie die IP-Adressen ein.</li> <li>e. Klicken Sie auf Senden.</li> </ul>
Schritt 3	<p>Wählen Sie Websicherheits-Manager &gt; Benutzerdefinierte und externe URL-Kategorien aus.</p> <ul style="list-style-type: none"> <li>a. Wählen Sie Kategorie hinzufügen aus.</li> <li>b. Geben Sie diese Informationen an.</li> </ul>

Einstellungen	Beschreibung
Kategorienname	Geben Sie einen Bezeichner für diese URL-Kategorie ein. Dieser Name wird angezeigt, wenn Sie den URL-Filter für Richtliniengruppen konfigurieren.
Listenreihenfolge	Geben Sie die Reihenfolge dieser Kategorie in der Liste der benutzerdefinierten URL-Kategorien an. Geben Sie "1" für die erste URL-Kategorie in der Liste ein.  Das URL-Filtermodul wertet eine Clientanforderung anhand der benutzerdefinierten URL-Kategorien in der angegebenen Reihenfolge aus.
Kategorie Typ	Wählen Sie Lokale benutzerdefinierte Kategorie aus.
Erweitert	In diesem Abschnitt können Sie reguläre Ausdrücke eingeben, um zusätzliche Adresssätze anzugeben.  Sie können reguläre Ausdrücke verwenden, um mehrere Adressen anzugeben, die den von Ihnen eingegebenen Mustern entsprechen.

c. Senden und bestätigen Sie die Änderungen.

#### Schritt 4


Wählen Sie Websicherheits-Manager > Entschlüsselungsrichtlinien aus.

- a. Erstellen einer neuen Entschlüsselungsrichtlinie
- b. Wählen Sie das Identifizierungsprofil aus, das Sie zur Umgehung des HTTPS-Datenverkehrs für bestimmte Anwendungen erstellt haben.
- c. Klicken Sie im Bedienfeld "Erweitert" auf den Link für URL-Kategorien.
- d. Klicken Sie in der Spalte Hinzufügen auf, um die in Schritt 3 erstellte benutzerdefinierte URL-Kategorie hinzuzufügen.
- e. Wählen Sie Fertig aus.
- f. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link für URL-Filterung.

	<p>g. Wählen Sie Passthrough aus.</p> <p>h. Senden und bestätigen Sie die Änderungen.</p> <p>(Optional) Sie können die %(Formatangabe) verwenden, um Informationen zum Zugriffsprotokoll anzuzeigen.</p>
--	--

## Webproxy-Umgehung für Webanforderungen konfigurieren

Wenn Sie die benutzerdefinierten URL-Kategorien zur Umgehungsliste des Proxys hinzugefügt haben, werden alle IP-Adressen und die Domännennamen der benutzerdefinierten URL-Kategorien sowohl für die Quelle als auch für das Ziel umgangen.

Schritt 1	Wählen Sie Websicherheits-Manager > Einstellungen umgehen aus.
Schritt 2	Klicken Sie auf Einstellungen für Umgehung bearbeiten.
Schritt 3	<p>Geben Sie die Adressen ein, für die Sie den Web-Proxy umgehen möchten.</p> <hr/> <p> Hinweis: Wenn Sie /0 als Subnetzmaske für eine beliebige IP in der Umgehungsliste konfigurieren, umgeht die Appliance den gesamten Web-Datenverkehr. In diesem Fall interpretiert die Appliance die Konfiguration als 0.0.0.0/0.</p>
Schritt 4	Wählen Sie die benutzerdefinierten URL-Kategorien aus, die Sie der Liste der Proxyumgehungen hinzufügen möchten.
Schritt 5	Senden und bestätigen Sie Ihre Änderungen.

 **Achtung:** Sie können die Umgehung des Webproxys für reguläre Ausdrücke nicht festlegen.

## Berichte

Auf der Seite "Reporting" >> URL-Kategorien wird eine kollektive Anzeige von URL-Statistiken bereitgestellt, die Informationen über die am häufigsten zugeordneten URL-Kategorien und die am häufigsten blockierten URL-Kategorien enthält.

Auf dieser Seite werden kategoriespezifische Daten zu Bandbreiteneinsparungen und Web-Transaktionen angezeigt.

Abschnitt	Beschreibung
Time Range (Dropdown-Liste)	Wählen Sie den Zeitraum für Ihren Bericht aus.
URL-Kategorien mit höchster Gesamtanzahl an Transaktionen	In diesem Abschnitt werden die wichtigsten URL-Kategorien, die auf der Website besucht werden, im Diagrammformat aufgeführt.
Häufigste URL-Kategorien nach gesperrten und mit Warnung versehenen Transaktionen	Listet die oberste URL auf, die eine Block- oder Warnaktion ausgelöst hat, die pro Transaktion in einem Diagrammformat aufgetreten ist.
Übereinstimmende URL-Kategorien	<p>Zeigt die Verteilung der Transaktionen nach URL-Kategorie während des angegebenen Zeitraums, zuzüglich der genutzten Bandbreite und der in jeder Kategorie verbrachten Zeit.</p> <p>Wenn der Anteil nicht kategorisierter URLs größer als 15-20 % ist, sollten Sie folgende Optionen in Betracht ziehen:</p> <ul style="list-style-type: none"> <li>• Für bestimmte lokalisierte URLs können Sie benutzerdefinierte URL-Kategorien erstellen und diese auf bestimmte Benutzer oder Gruppenrichtlinien anwenden.</li> <li>• Sie können nicht kategorisierte und falsch klassifizierte URLs zur Evaluierung und Aktualisierung der Datenbank an Cisco melden.</li> <li>• Überprüfen Sie, ob Web Reputation Filter und Anti-Malware Filter aktiviert sind.</li> </ul>

# URL-Categories

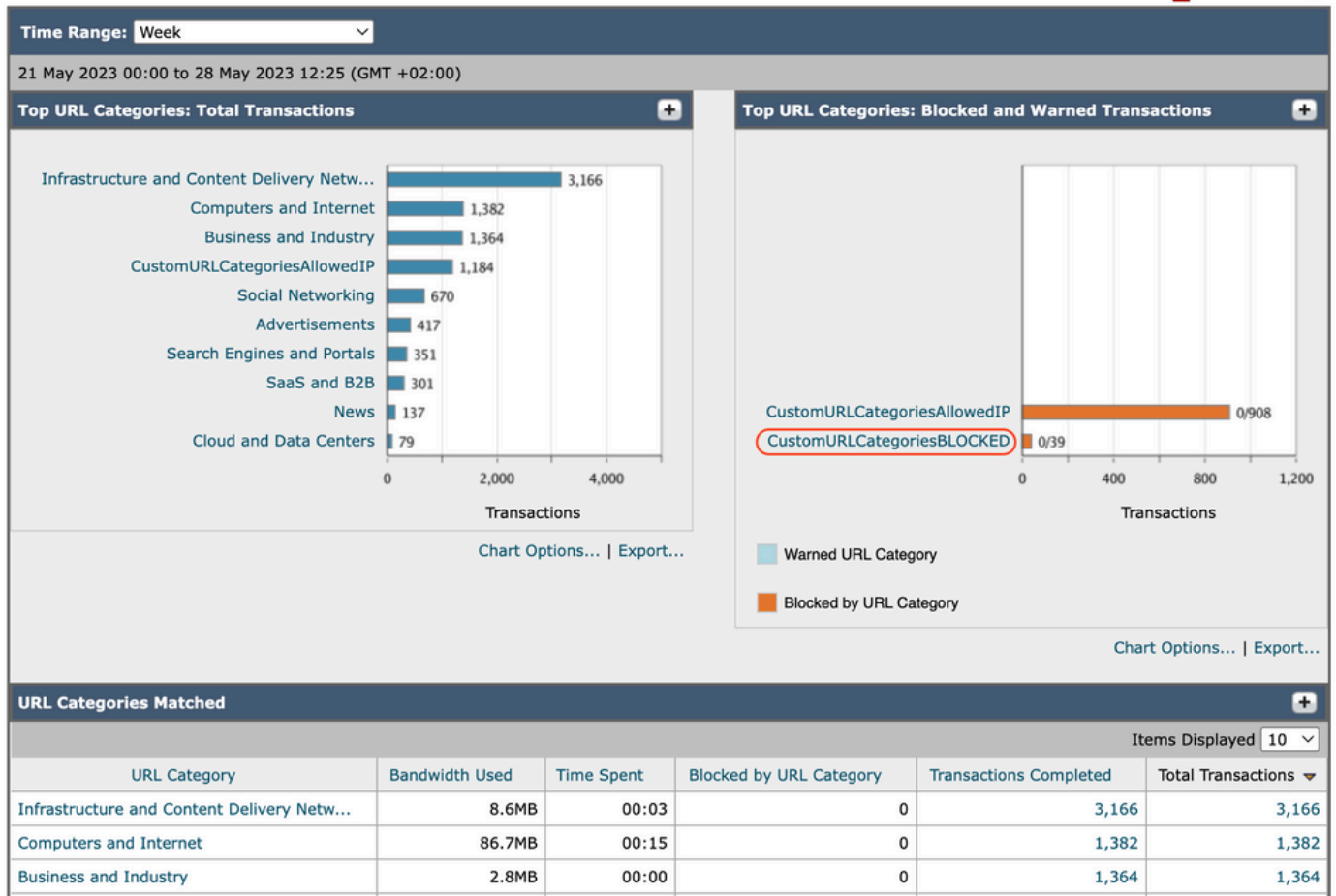


Bild-URL-Kategoriebericht

Sie können auf einen beliebigen Kategorienamen klicken, um weitere Details zu dieser Kategorie anzuzeigen, z. B. Übereinstimmende Domänen oder Benutzerliste.

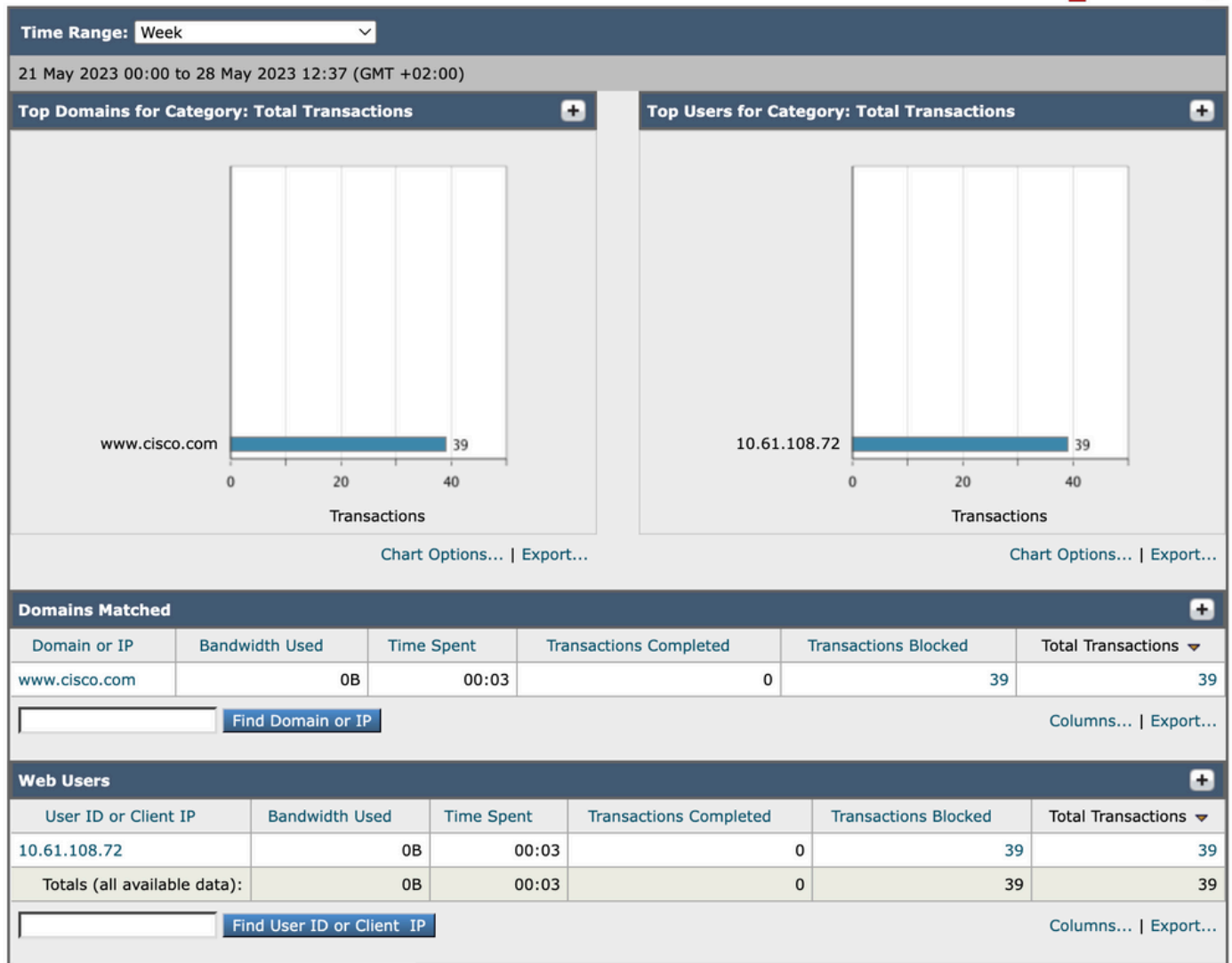


Bild - Detaillierte Berichtsseite

Die vordefinierten URL-Kategorien können in regelmäßigen Abständen automatisch auf der Websicherheits-Appliance aktualisiert werden.

Wenn diese Aktualisierungen erfolgen, werden alte Kategorienamen in Berichten so lange angezeigt, bis die mit den älteren Kategorien verknüpften Daten zu alt sind, um in die Berichte aufgenommen zu werden.

Berichtsdaten, die nach einer Aktualisierung des URL-Kategoriesatzes generiert werden, verwenden die neuen Kategorien, sodass Sie im gleichen Bericht sowohl alte als auch neue Kategorien sehen können.

In URL-Statistiken auf der Seite URL-Kategorien aus Berichten ist es wichtig zu wissen, wie diese Daten interpretiert werden:

Datentyp	Beschreibung
URL-Filterung umgangen	Stellt den blockierten Richtlinien-, Port- und Admin-Benutzer-Agent dar, der vor der URL-



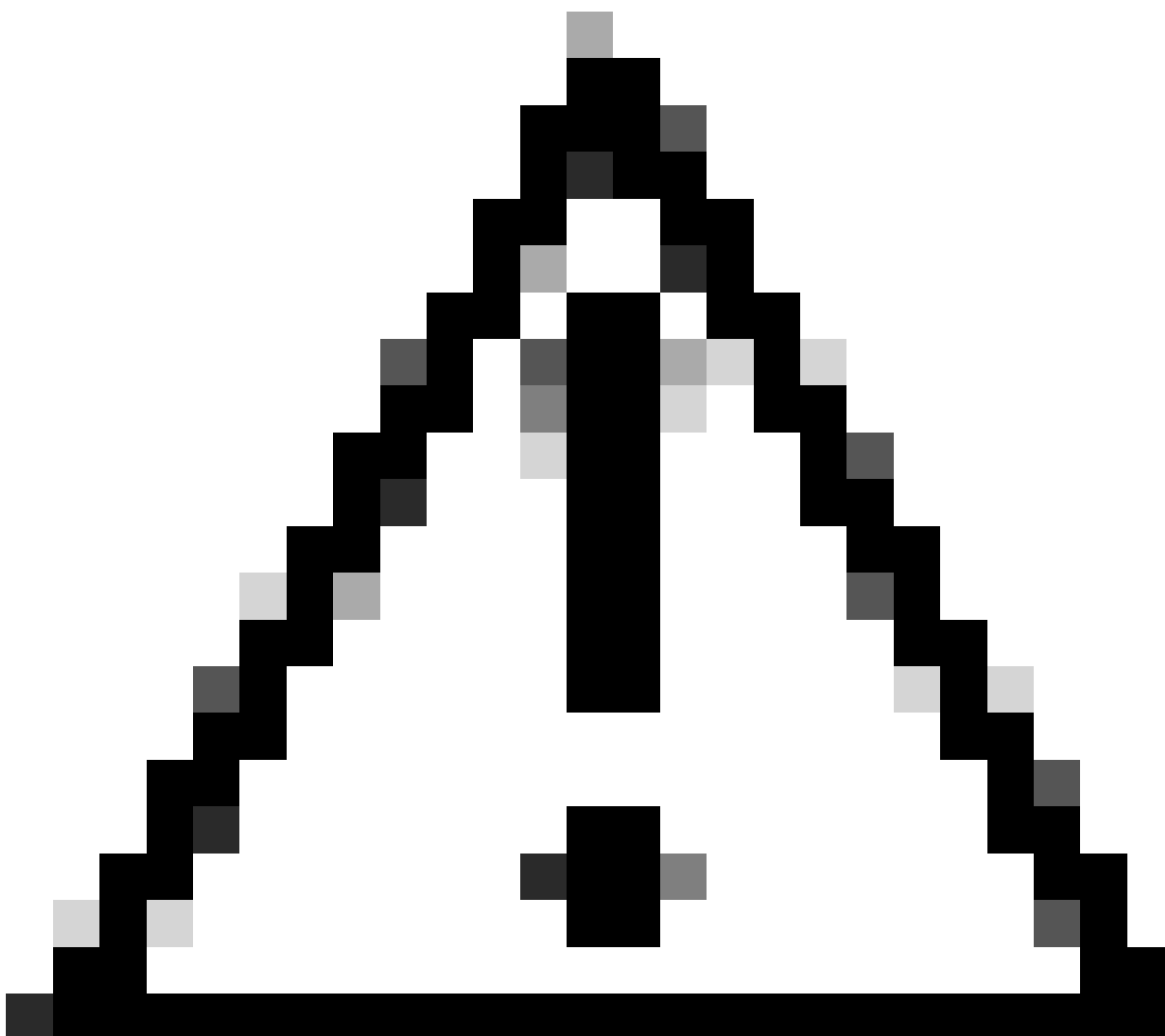
	Filterung auftritt.
Nicht kategorisierte URL	Stellt alle Transaktionen dar, für die das URL-Filtermodul abgefragt wird, aber keine Kategorie zugeordnet ist.

## Benutzerdefinierte URL-Kategorien im Zugriffsprotokoll anzeigen

Die sichere Web-Appliance verwendet die ersten vier Zeichen benutzerdefinierter URL-Kategorienamen, denen in den Zugriffsprotokollen "c\_" vorangestellt ist.

In diesem Beispiel lautet der Kategorienname CustomURLCategoriesBLOCKED, und in den Zugriffsprotokollen wird C\_Cust angezeigt:


```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



---

Achtung: Berücksichtigen Sie den benutzerdefinierten URL-Kategorienamen, wenn Sie Sawmill zum Analysieren der Zugriffsprotokolle verwenden. Wenn die ersten vier Zeichen der benutzerdefinierten URL-Kategorie ein Leerzeichen enthalten, kann Sawmill den Zugriffsprotokolleintrag nicht richtig analysieren. Verwenden Sie stattdessen nur unterstützte Zeichen in den ersten vier Zeichen.

---

 Tipp: Wenn Sie den vollständigen Namen einer benutzerdefinierten URL-Kategorie in die Zugriffsprotokolle aufnehmen möchten, fügen Sie den Zugriffsprotokollen die Formatangabe %XF hinzu.

---

Wenn für eine Webzugriffsrichtliniengruppe eine benutzerdefinierte URL-Kategorie auf Überwachung festgelegt ist und eine andere Komponente (z. B. die Webreputations-Filter oder das DVS-Modul (Different Verdicts Scanning)) die endgültige Entscheidung trifft, eine Anforderung für eine URL in der benutzerdefinierten URL-Kategorie zuzulassen oder zu blockieren, zeigt der Zugriffsprotokolleintrag für die Anforderung die vordefinierte URL-Kategorie anstelle der benutzerdefinierten URL-Kategorie an.

Weitere Informationen zum Konfigurieren benutzerdefinierter Felder in Zugriffsprotokollen finden Sie unter: [Konfigurieren von Leistungsparametern in Zugriffsprotokollen - Cisco](#)

## Fehlerbehebung

### Kategorie nicht zugeordnet

Aus den Zugriffsprotokollen können Sie sehen, dass die Anforderung zu welcher benutzerdefinierten URL-Kategorie gehört, wenn die Auswahl nicht wie erwartet erfolgt:

- Wenn die Anforderung in andere benutzerdefinierte URL-Kategorien eingeteilt ist, überprüfen Sie, ob in anderen Kategorien eine doppelte URL oder ein übereinstimmender regulärer Ausdruck vorhanden ist, oder verschieben Sie die benutzerdefinierte URL-Kategorie nach oben, und testen Sie sie erneut. Es ist besser, die angepasste benutzerdefinierte URL-Kategorie sorgfältig zu prüfen.
- Wenn die Anfrage in vordefinierte Kategorien kategorisiert ist, überprüfen Sie die Bedingungen in der vorhandenen benutzerdefinierten URL-Kategorie, wenn alle übereinstimmen, versuchen Sie, die IP-Adresse hinzuzufügen und zu testen, oder stellen Sie sicher, dass der Tippfehler und der richtige reguläre Ausdruck verwendet wird, falls vorhanden.

### Vordefinierte Kategorien sind nicht aktuell

Wenn die vordefinierten Kategorien nicht auf dem neuesten Stand sind oder in den Zugriffsprotokollen im URL-Kategorieabschnitt "err" angezeigt wird, stellen Sie sicher, dass TLSv1.2 für Updater aktiviert ist.

Um die SSL-Konfiguration des Updaters zu ändern, gehen Sie in der GUI wie folgt vor:

Schritt 1: Wählen Sie in System Administration (Systemverwaltung) SSL Configuration (SSL-Konfiguration) aus

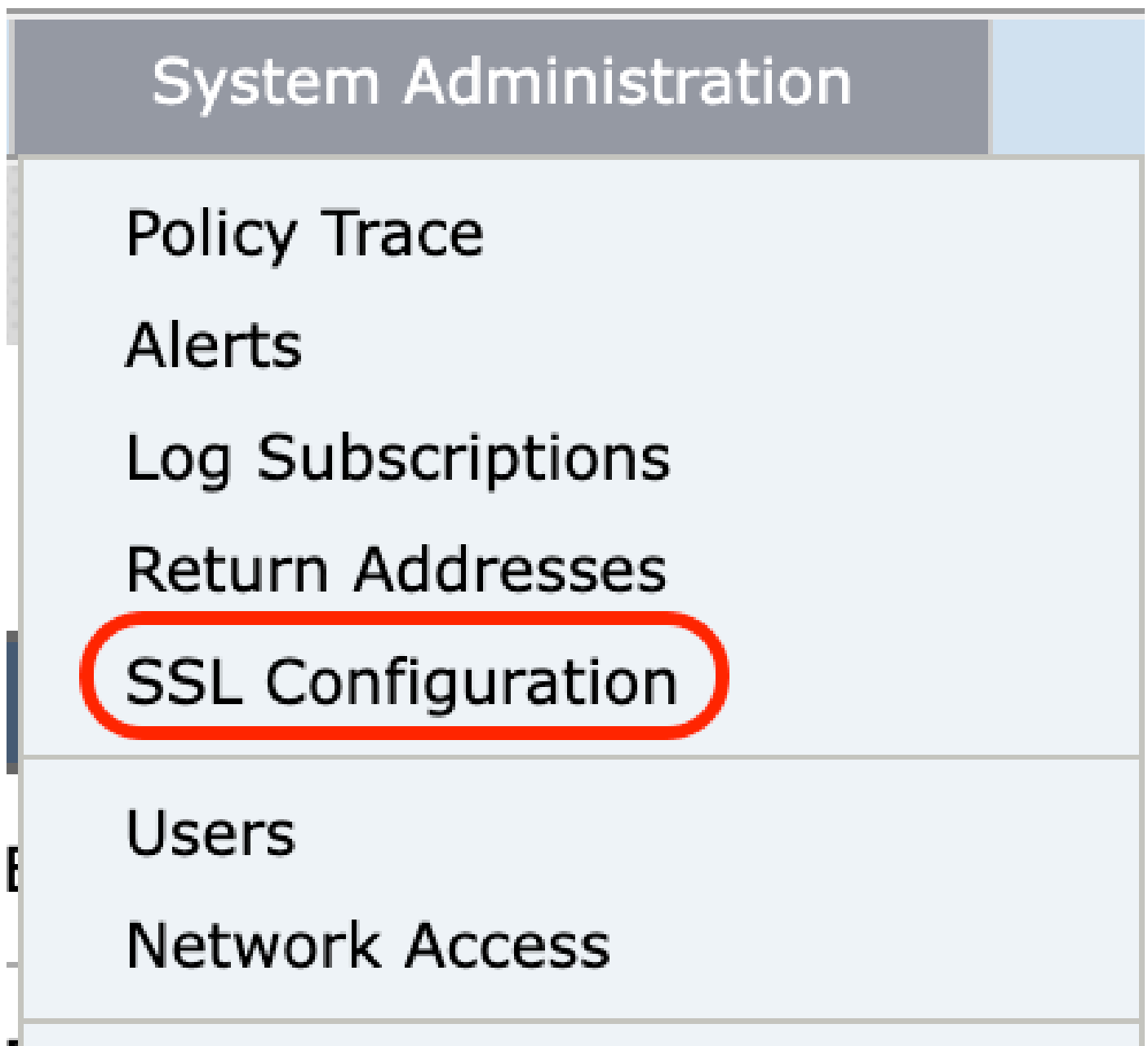


Image-/SSL-Konfiguration

Schritt 2: Wählen Sie Einstellungen bearbeiten.

Schritt 3: Wählen Sie im Abschnitt "Service aktualisieren" die Option TLSv1.2 aus.

## SSL Configuration

SSL Configuration	
<p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p>	
Appliance Management Web User Interface:	<p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Proxy Services:	<p>Proxy services include HTTPS Proxy and credential encryption for secure client.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.3 <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> <p><input checked="" type="checkbox"/> Disable TLS Compression (Recommended) TLS compression should be disabled for best security.</p> <p>Cipher(s) to Use: EECDH:DSS:RSA:NULL:!NULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA</p>
Secure LDAP Services:	<p>Secure LDAP services include Authentication, External Authentication, SaaS SSO, and Secure Mobility.</p> <p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
RADSEC Services:	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1</p>
Secure ICAP Services (External DLP):	<p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>
Update Service:	<p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p>

Cancel Submit

Image - Service TLSv1.2 aktualisieren

### Schritt 4: Änderungen übermitteln und bestätigen

Um die SSL-Konfiguration des Updaters zu ändern, gehen Sie in der CLI wie folgt vor:

Schritt 1: Führen Sie in der CLI `sslconfig` aus.

Schritt 2: Version eingeben und die Eingabetaste drücken

Schritt 3: Updater auswählen

Schritt 4: TLSv1.2 auswählen

Schritt 5: Drücken Sie die Eingabetaste, um den Assistenten zu beenden.

Schritt 6. Bestätigen Sie die Änderungen.

```
SWA_CLI> sslconfig
```

```
Disabling SSLv3 is recommended for best security.
```

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:

- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.

[> versions

SSL/TLS versions may be enabled or disabled for the following services:

- LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secure Client)
- Updater - Update Service
- WebUI - Appliance Management Web User Interface
- RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
- SICAP - Secure ICAP Service
- Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

	LDAPS	Updater	WebUI	RADSEC	SICAP	Proxy
TLSv1.0	N	N	N	N/A	N	N
TLSv1.1	Y	Y	N	Y	Y	N
TLSv1.2	N	N	Y	Y	Y	Y
TLSv1.3	N/A	N/A	N/A	N/A	N/A	Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services

[> 2

Currently enabled protocol(s) for Updater are TLSv1.1.

To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2

[> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y

Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.

## Referenz

[Best Practices-Richtlinien für Cisco Web Security Appliances - Cisco](#)

[BRKSEC-3303 \(Cisco Live\)](#)

[Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD \(Allgemeine Bereitstellung\) - Verbinden, Installieren und Konfigurieren \[Cisco Secure Web Appliance\] - Cisco](#)

## 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.