

Aangepaste URL-categorieën configureren in applicatie voor beveiligd web

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Aangepaste URL-categorieën](#)

[URL-categorieën voor live feed](#)

[Stappen voor Aangepaste URL-categorieën maken](#)

[Reguliere expressies gebruiken definiëren](#)

[Beperkingen en ontwerpproblemen](#)

[Aangepaste URL-categorieën gebruiken in beleid](#)

[Stappen om URL-filters voor toegangsbeleid te configureren](#)

[Stappen om URL-filters voor decryptie te configureren](#)

[Stappen om URL-filters voor gegevensbeveiligingsbeleidsgroepen te configureren](#)

[Stappen om het controleren van uploadaanvragen te configureren met aangepaste URL-categorieën](#)

[Stappen om ControlUpload-aanvragen in extern DLP-beleid te configureren](#)

[URL's voor bypass en doorgifte](#)

[Web Proxy-omzetting configureren voor webaanvragen](#)

[Rapporten](#)

[Aangepaste URL-categorieën in het toegangslogboek bekijken](#)

[Problemen oplossen](#)

[Categorie mismatched](#)

[Referentie](#)

Inleiding

Dit document beschrijft de structuur van Aangepaste Uniform Resource Locator (URL)-categorieën, in Secure Web Applicatie (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe proxy werkt.
- Beheer van Secure Web Appliance (SWA).

Cisco raadt u aan het volgende te doen:

- Physical of Virtual Secure Web Applicatie (SWA) geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- De setup-wizard is voltooid.

- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.


De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Aangepaste URL-categorieën

Met de URL-filterengine kunt u transacties filteren in beleid voor toegang, decryptie en gegevensbeveiliging. Wanneer u URL-categorieën voor beleidsgroepen vormt, kunt u acties voor aangepaste URL-categorieën configureren, als er categorieën worden gedefinieerd, en vooraf gedefinieerde URL-categorieën.

U kunt aangepaste en externe URL-categorieën voor live-feed maken die specifieke hostnamen en IP-adressen (Internet Protocol) beschrijven. Daarnaast kunt u URL-categorieën bewerken en verwijderen.

Wanneer u deze aangepaste URL-categorieën opneemt in dezelfde groep voor toegangsbeleid, decryptie of Cisco-gegevensbeveiligingsbeleid en verschillende acties aan elke categorie toewijst, heeft de actie van de hogere meegeleverde aangepaste URL-categorie voorrang.

 **Opmerking:** Als Domain Name System (DNS) meerdere IP's naar een website oplost en als een van die IP's op maat geblokkeerde lijst is, blokkeert de Web Security Applicatie de website voor alle IP's, ongeacht of deze niet in de op maat geblokkeerde lijst staan.

URL-categorieën voor live feed

Externe Live Feed Categorieën worden gebruikt om de lijst van URL's van specifieke site te halen, bijvoorbeeld om de Office 365 URL's van Microsoft te halen.

Als u de categorie Externe Live feed voor het categorietype selecteert wanneer u Aangepaste en externe URL-categorieën maakt en bewerkt, moet u de bestandsindeling voor de feed selecteren (Cisco Feed Format of Office 365 Feed Format) en vervolgens een URL naar de juiste feed-bestandsserver opgeven.

Hier is het formaat dat voor elk invoerbestand wordt verwacht:

- Cisco Feed Format - Dit moet een komma-gescheiden waardenbestand (.csv) zijn; dit is een tekstbestand met de extensie .csv. Elke ingang in het .csv bestand moet op een aparte regel staan, opgemaakt als adres/komma/adrestype (bijvoorbeeld: [www.cisco.com,site](http://www.cisco.com/site) of ad2.*\com,regex). Geldige adrestypen zijn site en regex.

Hier volgt een fragment uit een CSV-bestand met 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 - Dit is een XML-bestand dat zich op een Microsoft Office 365-server bevindt, of een lokale server waaraan u het bestand hebt opgeslagen. Het wordt geleverd door de Office 365-dienst en kan niet worden gewijzigd.

De netwerkadressen in het bestand worden omgeven door XML-tags, deze structuur: producten > product > adreslijst > adres. In de huidige implementatie kan een "adrestype" IPv6, IPv4 of URL zijn [waaronder domeinen en reguliere expressies (regex) patronen].

Hier is een fragment van een Office 365-feed:

```
<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>
```

 Opmerking: neem <http://> of <https://> niet op als onderdeel van een sitevermelding in het bestand, of er treedt een fout op. Met andere woorden: www.cisco.com wordt correct geparsed, terwijl <http://www.cisco.com> een fout oplevert

Stappen om aangepaste URL-categorieën te maken

Stap 1. Kies Web Security Manager > Aangepaste en externe URL-categorieën.

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

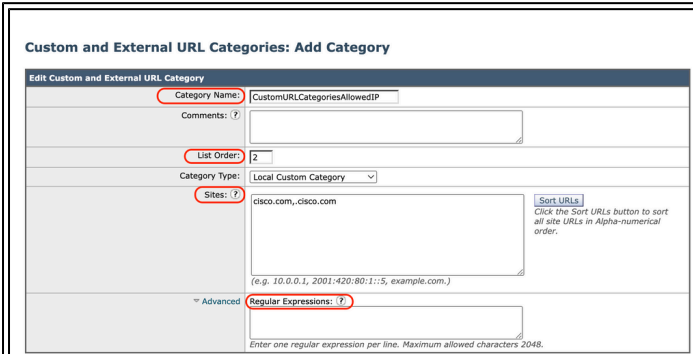
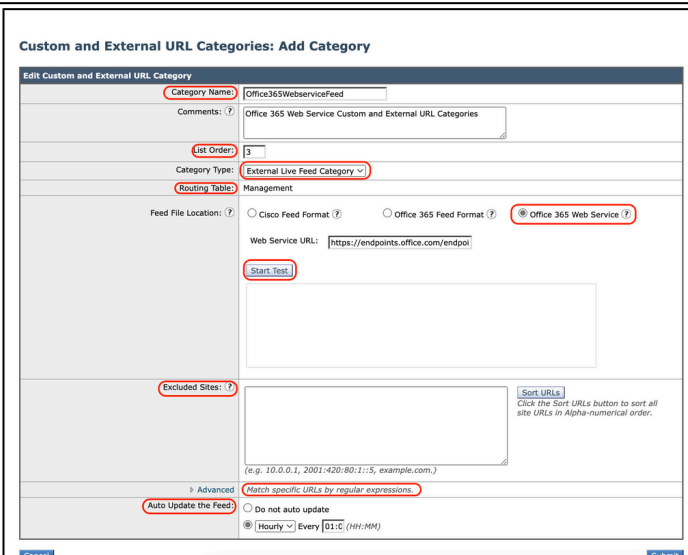
: Voer een id in voor deze URL-categorie. Deze naam verschijnt wanneer u URL filter voor beleidsgroepen vormt.

- Lijstvolgorde: Geef de volgorde van deze categorie op in de lijst met aangepaste URL-categorieën. Typ "1" voor de eerste URL-categorie in de lijst.

De URL filter engine evalueert een client verzoek aan de aangepaste URL categorieën in de opgegeven volgorde.

 **Opmerking:** Wanneer de URL-filterengine een URL-categorie aanpast aan de URL in een clientaanvraag, evalueert deze eerst de URL aan de hand van de aangepaste URL-categorieën die in de beleidsgroep zijn opgenomen. Als de URL in de aanvraag niet overeenkomt met een meegeleverde aangepaste categorie, vergelijkt de URL-filterengine deze met de vooraf gedefinieerde URL-categorieën. Als de URL niet overeenkomt met de meegeleverde aangepaste of vooraf gedefinieerde URL-categorieën, wordt de aanvraag niet gecategoriseerd.

- Categorietype: Kies lokale aangepaste categorie of externe live feed categorie.
- Routing Table: Kies Beheer of Gegevens. Deze keuze is alleen beschikbaar als "gesplitste routing" is ingeschakeld, dat wil zeggen dat deze niet beschikbaar is bij lokale aangepaste categorieën.

 <p>afbeelding - Lokale aangepaste URL-categorie</p>	 <p>Afbeelding - Aangepaste URL-categorie configureren Feeds</p>
Lokale aangepaste categorie	Extern levend diervoeder

Reguliere expressies gebruiken definiëren


De Secure Web Applicatie gebruikt een syntaxis van reguliere expressies die enigszins afwijkt van de syntaxis van reguliere expressies die wordt gebruikt door andere Velocity-patroonimplementaties.


Bovendien ondersteunt het apparaat geen achterwaartse schuine streep om aan een voorwaartse schuine streep te ontsnappen. Als u een voorwaartse slash in een reguliere expressie moet

gebruiken, typt u de voorwaartse slash zonder een achterwaartse slash.

 Opmerking: Technisch gebruikt AsyncOS voor Web de Flex regular expressie analyzer

Om uw reguliere expressies te testen kunt u deze link gebruiken: [flex lint - Regex Tester/Debugger](#)

 Waarschuwing: Reguliere expressies die meer dan 63 tekens teruggeven, mislukken en veroorzaken een fout bij het ongeldig invoeren van de code. Zorg ervoor dat u reguliere expressies vormt die niet meer dan 63 tekens kunnen retourneren

 Waarschuwing: Reguliere expressies die uitgebreide tekenovereenkomsten uitvoeren, verbruiken resources en kunnen de systeemprestaties beïnvloeden. Daarom kunnen reguliere expressies voorzichtig worden toegepast.

U kunt reguliere expressies op deze locaties gebruiken:

- Aangepaste URL-categorieën voor toegangsbeleid. Wanneer u een aangepaste URL-categorie maakt die u met toegangsbeleidsgroepen kunt gebruiken, kunt u gebruikmaken van reguliere expressies om meerdere webservers op te geven die overeenkomen met het patroon dat u invoert.


- Aangepaste gebruikersagents voor blokkering. Wanneer u de te blokkeren toepassingen voor een groep Toegangsbeleid bewerkt, kunt u gebruikmaken van reguliere expressies om specifieke te blokkeren gebruikersagents in te voeren.

 Tip: u kunt de webproxy-omzeilen voor Reguliere expressies niet instellen.

Dit is de lijst met tekenklassen in Flex Regular Expression

Tekensymbolen	
.	om het even welk karakter behalve nieuwe lijn
\w \d \s	woord, cijfer, witte ruimte
\W \D \S	geen woord, cijfer, witte ruimte
[abc]	een van de delen a, b of c
[^abc]	niet a, b of c
[a-g]	teken tussen a en g
Ankers	
^abc\$	begin/eind van de string
\b	woordgrens
Ontsnapte tekens	
\. * \	ontsnapte speciale tekens
\t \n \r	tab, linefeed, wagenterugloop

\u00A9	unicode ontsnapt ©
Groepen en Zoeken	
abc)	opnamegroep
\1	terug naar groep #1
(?:abc)	niet-opnamegroep
(?=abc)	positieve blik op de toekomst
(?!abc)	negatieve blik op de toekomst
Kwalificaties en alternatieven	
a* a+ a?	0 of meer, 1 of meer, 0 of 1
a {5} a {2}	precies vijf, twee of meer
a{1,3}	tussen één en drie
a+? a{2,}?	zo min mogelijk
ab cd	match ab of cd

 Waarschuwing: wees voorzichtig met niet-ontsnapte punten in lange patronen, en vooral in het midden van langere patronen en wees voorzichtig met dit meta-teken (Star *), vooral in samenhang met het puntteken. Om het even welk patroon bevat een niet-ontsnapte punt dat meer dan 63 karakters terugkeert nadat de punt gehandicapt is.

Altijd ontsnappen * (ster) en . (punt) met \ (backslash) zoals * en \.

Als we .cisco.local gebruiken in de reguliere expressie is het domein Xcisco.local ook een match.

Het niet-ontsnapte karakter beïnvloedt de prestaties en het leidt tot traagheid tijdens Web het Doorbladeren. Dit is omdat de patroon-aanpassing motor door duizenden of miljoenen mogelijkheden moet gaan tot het vinden van een gelijke voor de juiste ingang ook kan het sommige veiligheidszorgen met betrekking tot de gelijkaardige URLs voor toegestaan Beleid hebben

U kunt de opdrachtregel interface (CLI) optie advanced proxyconfig > diversen > Wilt u URL kleine case conversie inschakelen voor snelheid regex, om standaard regex conversie in te schakelen of uit te schakelen naar kleine case voor case-ingevoelige overeenkomsten. Gebruik dit als u problemen hebt met de gevoeligheid van de case.

Beperkingen en ontwerproblemen

- U kunt niet meer dan 30 Externe Live Feed bestanden in deze URL categorie definities gebruiken, en elk bestand mag niet meer dan 5000 items bevatten.
- Als het aantal externe voedingangen toeneemt, leidt dit tot een verslechtering van de prestaties.
- Het is mogelijk om hetzelfde adres te gebruiken in meerdere aangepaste URL-categorieën, maar de volgorde waarin de categorieën worden weergegeven is relevant.

Als u deze categorieën in hetzelfde beleid opneemt en voor elke categorie verschillende acties definieert, wordt de actie die is gedefinieerd voor de categorie die het hoogst staat in de tabel met

aangepaste URL-categorieën toegepast.

- Wanneer een native File Transfer Protocol (FTP)-verzoek transparant wordt doorgestuurd naar de FTP-proxy, bevat het geen Hostname-informatie voor de FTP-server, alleen zijn IP-adres.

Daarom komen sommige vooraf gedefinieerde URL-categorieën en webreputatiefilters die alleen informatie over Hostname hebben, niet overeen met native FTP-verzoeken, zelfs als de verzoeken bestemd zijn voor die servers.

Als u de toegang tot deze sites wilt blokkeren, moet u aangepaste URL-categorieën voor hen maken om hun IP-adressen te gebruiken.

- Een niet-gecategoriseerde URL is een URL die niet overeenkomt met een vooraf gedefinieerde URL-categorie of een aangepaste URL-categorie

Aangepaste URL-categorieën gebruiken in beleid

Met de URL-filterengine kunt u transacties filteren in beleid voor toegang, decryptie en gegevensbeveiliging. Wanneer u URL-categorieën voor beleidsgroepen vormt, kunt u acties voor aangepaste URL-categorieën configureren, als er categorieën worden gedefinieerd, en vooraf gedefinieerde URL-categorieën.

Stappen om URL-filters voor toegangsbeleid te configureren

Stap 1. Kies Web Security Manager > Toegangsbeleid.

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

Klik op de koppeling in de tabel Beleid onder de kolom URL-filter voor de beleidsgroep die u wilt bewerken.

Access Policies

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

Afbeelding - Aangepaste categorie toevoegen aan toegangsbeleid

Stap 3. (optioneel) In de sectie Aangepaste URL-categoriefiltering kunt u aangepaste URL-categorieën toevoegen waarop u actie kunt ondernemen in dit beleid:

a) Klik op Aangepaste categorieën selecteren.

Access Policies: URL Filtering: Access Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Afbeelding-Selecteer Aangepaste URL-categorie

b) Kies welke aangepaste URL-categorieën in dit beleid moeten worden opgenomen en klik op Toepassen.

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

Aangepaste categorieën selecteren om in beleid op te nemen

Kies welke aangepaste URL-categorieën de URL-filterengine moet vergelijken met de clientaanvraag.

De URL filter engine vergelijkt client aanvragen met de meegeleverde aangepaste URL categorieën en negeert uitgesloten aangepaste URL categorieën.

De URL filter engine vergelijkt de URL in een client aanvraag met de aangepaste URL categorieën voor vooraf gedefinieerde URL categorieën.

De aangepaste URL-categorieën die in het beleid zijn opgenomen, worden weergegeven in het gedeelte Eigen URL-categorie filtering.

Stap 4. Kies in het gedeelte Aangepaste URL-categorie filtering een actie voor elke meegeleverde aangepaste URL-categorie.



Afbeelding - Actie kiezen voor aangepaste categorie

Actie	Beschrijving
Algemene instellingen gebruiken	Gebruikt de actie voor deze categorie in de Global Policy Group. Dit is de standaardactie voor door de gebruiker gedefinieerde beleidsgroepen. Is alleen van toepassing op door de gebruiker gedefinieerde beleidsgroepen.
Block (blokkeren)	De webproxy ontkent transacties die overeenkomen met deze instelling.
Doorsturen	Richt verkeer dat oorspronkelijk voor een URL in deze categorie is bestemd om naar een door u opgegeven locatie te worden geleid. Wanneer u deze actie kiest, wordt het veld Omleiden naar weergegeven. Voer een URL in waarnaar u al het verkeer wilt doorsturen.
Allow (toestaan)	Altijd staat client aanvragen voor websites in deze categorie toe. Toegestane verzoeken omzeilen alle verdere filters en Malware scans. Gebruik deze instelling alleen voor vertrouwde websites. U kunt deze instelling gebruiken voor interne sites.
Monitor (bewaken)	De Web Proxy staat noch blokkeert het verzoek toe. In plaats daarvan, blijft het het cliëntverzoek tegen andere instellingen van de beleidsgroepcontrole, zoals de filter van de Webreputatie evalueren.

Actie	Beschrijving
Waarschuwen	De webproxy blokkeert het verzoek en geeft een waarschuwingspagina weer, maar stelt de gebruiker in staat om door te gaan door op een hypertextlink op de waarschuwingspagina te klikken.
op quota gebaseerd	Aangezien een individuele gebruiker of het volume of de tijdquota's benadert die u hebt gespecificeerd, wordt een waarschuwing weergegeven. Wanneer een quota wordt voldaan aan, wordt een blokpagina weergegeven. .
tijdgebaseerd	De Web Proxy blokkeert of controleert het verzoek tijdens de tijdbereiken die u specificeert.

Stap 5. In het gedeelte Categoriefilter voor voorgedefinieerde URL kiest u een van deze acties voor elke categorie:

- Algemene instellingen gebruiken
- Monitor (bewaken)
- Waarschuwen
- Block (blokkeren)
- tijdgebaseerd
- op quota gebaseerd

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			<input checked="" type="checkbox"/>			
Astrology					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Afbeelding - Selecteer Actie voor vooraf gedefinieerde categorie

Stap 6. In de sectie Uncategorized URLs, kies de actie om voor cliëntverzoeken aan websites te nemen die niet in een vooraf bepaalde of douane URL categorie vallen. Deze instelling bepaalt ook de standaardactie voor nieuwe en samengevoegde categorieën resulteert uit URL-categorieën die worden bijgewerkt.

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

Afbeelding - Actie kiezen voor niet-gecategoriseerde URL

Stap 7. Veranderingen verzenden en doorvoeren.

Stappen om URL-filters te configureren voor decryptie-beleid

Stap 1. Kies Web Security Manager > Decryptie Beleid.

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

Klik op de link in de tabel met beleidsregels onder de kolom URL-filtering voor de beleidsgroep die u wilt bewerken.

Decryption Policies

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

Edit Policy Order...

Afbeelding - URL-filter kiezen

Stap 3. (Optioneel) In de sectie Aangepaste URL-categoriefiltering kunt u aangepaste URL-categorieën toevoegen waarop u actie kunt ondernemen in dit beleid:

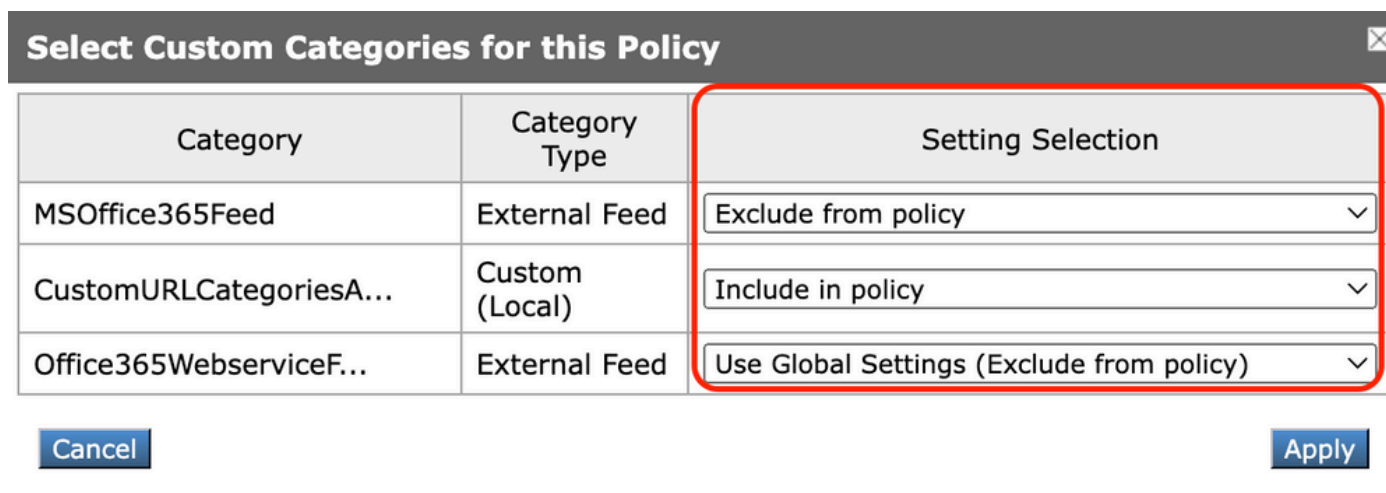
- a. Klik op Aangepaste categorieën selecteren.

Decryption Policies: URL Filtering: DecryptionPolicy



Afbeelding - Aangepaste categorieën kiezen

- b. Kies welke aangepaste URL-categorieën in dit beleid moeten worden opgenomen en klik op Toepassen.



Aangepaste categorieën selecteren om in beleid op te nemen

Kies welke aangepaste URL-categorieën de URL-filterengine moet vergelijken met de clientaanvraag.

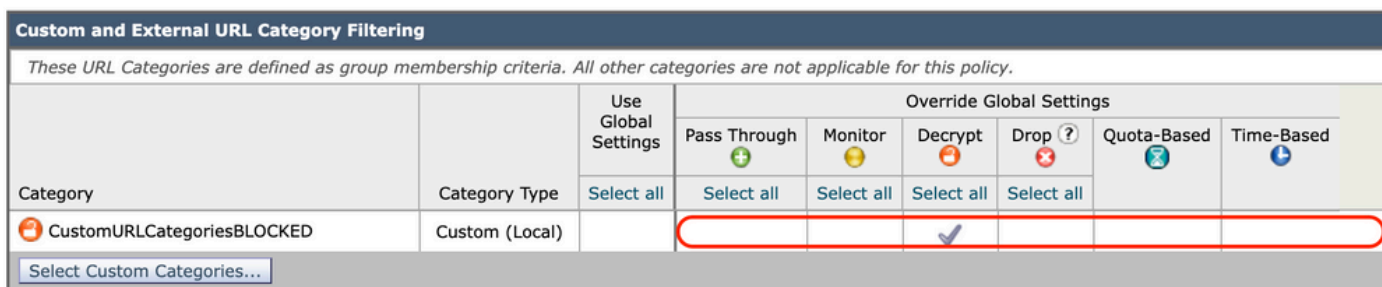
De URL filter engine vergelijkt client aanvragen met de meegeleverde aangepaste URL

categorieën en negeert uitgesloten aangepaste URL categorieën.

De URL filter engine vergelijkt de URL in een client aanvraag met de aangepaste URL categorieën voor vooraf gedefinieerde URL categorieën.

De aangepaste URL-categorieën die in het beleid zijn opgenomen, worden weergegeven in het gedeelte Eigen URL-categorie filtering.

Stap 4. Kies een actie voor elke aangepaste en vooraf gedefinieerde URL-categorie.



Afbeelding - Kies Actie voor decryptie Beleid

Actie	Beschrijving
Algemene instelling gebruiken	<p>Gebruikt de actie voor deze categorie in de groep wereldwijd decryptie beleid. Dit is de standaardactie voor door de gebruiker gedefinieerde beleidsgroepen.</p> <p>Is alleen van toepassing op door de gebruiker gedefinieerde beleidsgroepen.</p> <p>Wanneer een aangepaste URL-categorie is uitgesloten in het globale decryptie beleid, dan is de standaardactie voor de opgenomen aangepaste URL-categorieën in door de gebruiker gedefinieerd decryptie beleid Monitor in plaats van Gebruik Global Settings. U kunt geen globale instellingen gebruiken als een aangepaste URL-categorie is uitgesloten in het algemene decryptie beleid.</p>
Doorlopen	Gaat door de verbinding tussen de client en de server zonder inspectie van de verkeersinhoud.
Monitor (bewaken)	De Web Proxy staat noch blokkeert het verzoek toe. In plaats daarvan, blijft het het cliëntverzoek tegen andere instellingen van de beleidsgroepcontrole, zoals de filter van de Webreputatie evalueren.
ontcijferen	Staat de verbinding toe, maar inspecteert de verkeersinhoud. Het apparaat decrypteert het verkeer en past het Toegangsbeleid op het gedecrypteerde verkeer toe alsof het een duidelijke verbinding van de Hypertext Transfer Protocol (HTTP) was. Wanneer de verbinding wordt gedecrypteerd en het Toegepaste


Actie	Beschrijving
	Beleid van de Toegang, kunt u het verkeer op Malware scannen.
Afwijzing	Laat de verbinding vallen en geeft de verbindingsaanvraag niet door aan de server. Het apparaat geeft de gebruiker niet door dat de verbinding is verbroken.

Stap 5. In de sectie Uncategorized URLs, kies de actie om voor cliëntverzoeken aan websites te nemen die niet in een vooraf bepaalde of douane URL categorie vallen.

Deze instelling bepaalt ook de standaardactie voor nieuwe en samengevoegde categorieën resulteert uit URL-categorieën die worden bijgewerkt.

Afbeelding - Ongecategoriseerd decryptie Beleid

Stap 6. Veranderingen verzenden en doorvoeren.

 Let op: als u een bepaalde URL-categorie wilt blokkeren voor HTTPS-verzoeken (Hypertext Transfer Protocol Secure), kiest u om die URL-categorie te decrypteren in de groep Decryptie Beleid en kiest u om dezelfde URL-categorie te blokkeren in de groep Toegangsbeleid.

Stappen om URL-filters voor gegevensbeveiligingsbeleidsgroepen te configureren

Stap 1. Kies Web Security Manager > Cisco Data Security Security.

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

Klik op de link in de tabel met beleidsregels onder de kolom URL-filtering voor de beleidsgroep die u wilt bewerken.

Cisco Data Security

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

Edit Policy Order...

Afbeelding - Data Security kiest URL-filter

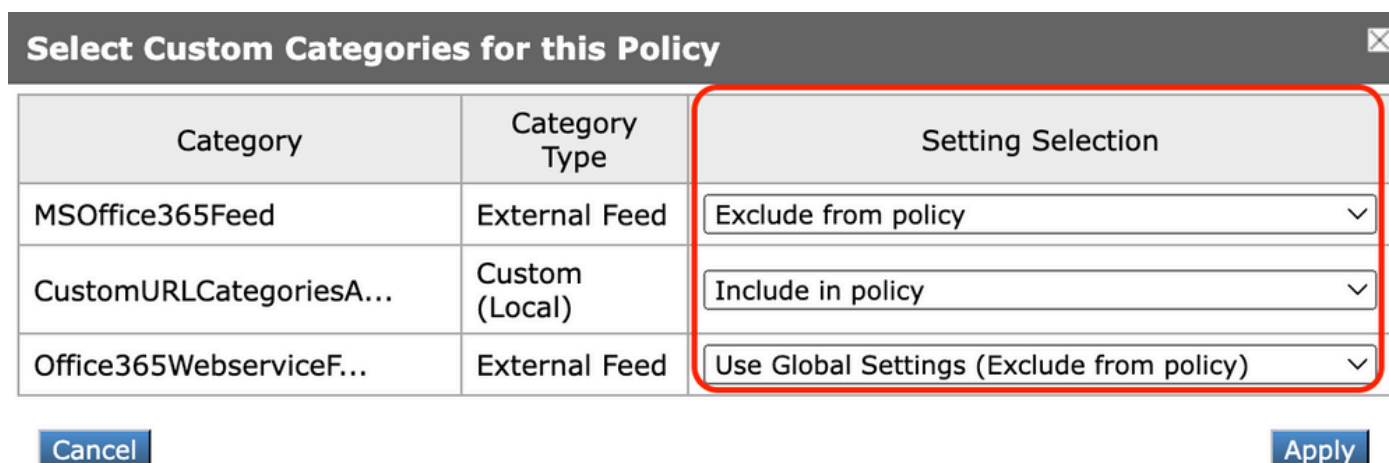
Stap 3. (Optioneel) In de sectie Aangepaste URL-categoriefiltering kunt u aangepaste URL-categorieën toevoegen waarop u actie kunt ondernemen in dit beleid:

- a. Klik op Aangepaste categorieën selecteren.



Afbeelding - Aangepast veld selecteren

- b. Kies welke aangepaste URL-categorieën in dit beleid moeten worden opgenomen en klik op Toepassen.



Aangepaste categorieën selecteren om in beleid op te nemen

Kies welke aangepaste URL-categorieën de URL-filterengine moet vergelijken met de clientaanvraag.

De URL filter engine vergelijkt client aanvragen met de meegeleverde aangepaste URL categorieën en negeert uitgesloten aangepaste URL categorieën.

De URL filter engine vergelijkt de URL in een client aanvraag met de aangepaste URL categorieën voor vooraf gedefinieerde URL categorieën.

De aangepaste URL-categorieën die in het beleid zijn opgenomen, worden weergegeven in het gedeelte Eigen URL-categorie filtering.

Stap 4. In de sectie Aangepaste URL-categorie filtering kiest u een actie voor elke aangepaste URL-categorie.

Custom and External URL Category Filtering					
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>					
Category	Category Type	Use Global Settings	Override Global Settings		
			Allow ? +	Monitor ⚠	Block ✖
		Select all	Select all	Select all	Select all
✖ CustomURLCategoriesBLOCKED	Custom (Local)	—	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Select Custom Categories...					

Afbeelding - Data Security Kies actie

Actie	Beschrijving
Algemene instelling gebruiken	<p>Gebruikt de actie voor deze categorie in de Global Policy Group. Dit is de standaardactie voor door de gebruiker gedefinieerde beleidsgroepen.</p> <p>Is alleen van toepassing op door de gebruiker gedefinieerde beleidsgroepen.</p> <p>Wanneer een aangepaste URL-categorie is uitgesloten in het wereldwijde Cisco-gegevensbeveiligingsbeleid, is de standaardactie voor de meegeleverde aangepaste URL-categorieën in door de gebruiker gedefinieerd Cisco-gegevensbeveiligingsbeleid Monitor in plaats van Globale instellingen gebruiken. U kunt niet kiezen voor Globale instellingen gebruiken als een aangepaste URL-categorie is uitgesloten in het algemene Cisco-beveiligingsbeleid voor gegevens.</p>
Allow (toestaan)	<p>Stelt altijd uploadverzoeken voor websites in deze categorie in. Is alleen van toepassing op aangepaste URL-categorieën.</p> <p>Toegestane verzoeken omzeilen alle verdere gegevensbeveiligingsscan en het verzoek wordt beoordeeld aan de hand van het toegangsbeleid.</p> <p>Gebruik deze instelling alleen voor vertrouwde websites. U kunt deze instelling gebruiken voor interne sites.</p>
Monitor (bewaken)	<p>De Web Proxy staat noch blokkeert het verzoek toe. In plaats daarvan blijft het de uploadaanvraag evalueren aan de hand van andere beleidsgroepcontrole-instellingen, zoals web reputation filter.</p>

Actie	Beschrijving
Block (blokkeren)	De webproxy ontkent transacties die overeenkomen met deze instelling.

Stap 5. In het gedeelte Category-filtering van voorgedefinieerde URL kiest u een van deze acties voor elke categorie:

- Algemene instellingen gebruiken
- Monitor (bewaken)
- Block (blokkeren)

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"/>

Afbeelding - Vooraf gedefinieerde URL voor gegevensbeveiliging Kies actie

Stap 6. In de sectie Uncategorized URLs, kies de actie om voor uploadverzoeken aan websites te nemen die niet in een vooraf bepaalde of aangepaste URL categorie vallen.

Deze instelling bepaalt ook de standaardactie voor nieuwe en samengevoegde categorieën resulteert uit URL-categorieën die worden bijgewerkt.

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"/>

Afbeelding - Gecategoriseerd voor gegevensbeveiliging

Stap 7. Veranderingen verzenden en doorvoeren.

⚠️ Waarschuwing: als u niet de maximale grootte van een bestand uitschakelt, blijft Web Security Appliance de maximale grootte van een bestand valideren wanneer de opties Toestaan of Monitoren zijn geselecteerd in URL-filtering.

Stappen om het controleren van uploadaanvragen te configureren met aangepaste URL-categorieën

Elk uploadverzoek wordt toegewezen aan een beleidsgroep "Uitgaande Malware Scanning" en erft de controle-instellingen van die beleidsgroep.

Nadat de Web Proxy de uploadverzoekkopregels ontvangt, heeft het de informatie die nodig is om te beslissen of het de aanvraaginstantie moet scannen.

De DVS engine scant het verzoek en geeft een oordeel terug aan de Web Proxy. De blokpagina wordt weergegeven aan de eindgebruiker, indien van toepassing.

Stap 1	Kies Web Security Manager > Uitgaande Malware Scannen.								
Stap 2	Klik in de kolom Bestemmingen op de link voor de beleidsgroep die u wilt configureren.								
Stap 3	Selecteer in het gedeelte Bestemmingsinstellingen bewerken de optie "Bestemmingen definiëren en aangepaste instellingen scannen" in het uitrolmenu.								
Stap 4	Selecteer in het gedeelte Bestemmingen voor scannen een van de volgende opties:								
	<table border="1"> <thead> <tr> <th>Optioneel</th> <th>Beschrijving</th> </tr> </thead> <tbody> <tr> <td>Scan geen uploads</td> <td>De DVS engine scant geen uploadverzoeken. Alle uploadverzoeken worden beoordeeld aan de hand van het toegangsbeleid</td> </tr> <tr> <td>Alle uploads scannen</td> <td>De DVS engine scant alle uploadverzoeken. Het uploadverzoek wordt geblokkeerd of beoordeeld volgens het Toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan</td> </tr> <tr> <td>Uploaden scannen naar opgegeven aangepaste URL-categorieën</td> <td>De DVS engine scant uploadverzoeken die behoren tot specifieke aangepaste URL-categorieën. Het uploadverzoek wordt geblokkeerd of geëvalueerd aan de hand van het toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan. Klik op Aangepaste categorieën bewerken om de te scannen URL-categorieën te selecteren</td> </tr> </tbody> </table>	Optioneel	Beschrijving	Scan geen uploads	De DVS engine scant geen uploadverzoeken. Alle uploadverzoeken worden beoordeeld aan de hand van het toegangsbeleid	Alle uploads scannen	De DVS engine scant alle uploadverzoeken. Het uploadverzoek wordt geblokkeerd of beoordeeld volgens het Toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan	Uploaden scannen naar opgegeven aangepaste URL-categorieën	De DVS engine scant uploadverzoeken die behoren tot specifieke aangepaste URL-categorieën. Het uploadverzoek wordt geblokkeerd of geëvalueerd aan de hand van het toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan. Klik op Aangepaste categorieën bewerken om de te scannen URL-categorieën te selecteren
	Optioneel	Beschrijving							
	Scan geen uploads	De DVS engine scant geen uploadverzoeken. Alle uploadverzoeken worden beoordeeld aan de hand van het toegangsbeleid							
Alle uploads scannen	De DVS engine scant alle uploadverzoeken. Het uploadverzoek wordt geblokkeerd of beoordeeld volgens het Toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan								
Uploaden scannen naar opgegeven aangepaste URL-categorieën	De DVS engine scant uploadverzoeken die behoren tot specifieke aangepaste URL-categorieën. Het uploadverzoek wordt geblokkeerd of geëvalueerd aan de hand van het toegangsbeleid, afhankelijk van de uitspraak van de DVS-machinescan. Klik op Aangepaste categorieën bewerken om de te scannen URL-categorieën te selecteren								
Stap 5	Verzend uw wijzigingen.								

Stap 6	Klik in de kolom Anti-Malware Filtering op de link voor de beleidsgroep.
Stap 7	Selecteer in het gedeelte Anti-Malware-instellingen de optie Aangepaste anti-Malware-instellingen definiëren.
Stap 8	Selecteer in de sectie Cisco DVS Anti-Malware Settings welke anti-malware scanprogramma's u voor deze beleidsgroep wilt inschakelen.
Stap 9	In de sectie Malware Categorieën, kies of u de verschillende malware categorieën wilt controleren of blokkeren. Welke categorieën in deze sectie worden vermeld, is afhankelijk van de scanmotoren die u inschakelt.
Stap 10	Veranderingen verzenden en doorvoeren.

Stappen om controle te configureren en uploadaanvragen in extern DLP-beleid

Zodra de Web Proxy de uploadverzoekkopregels ontvangt, heeft het de informatie die nodig is om te beslissen of het verzoek naar het externe DLP-systeem voor scan kan gaan.

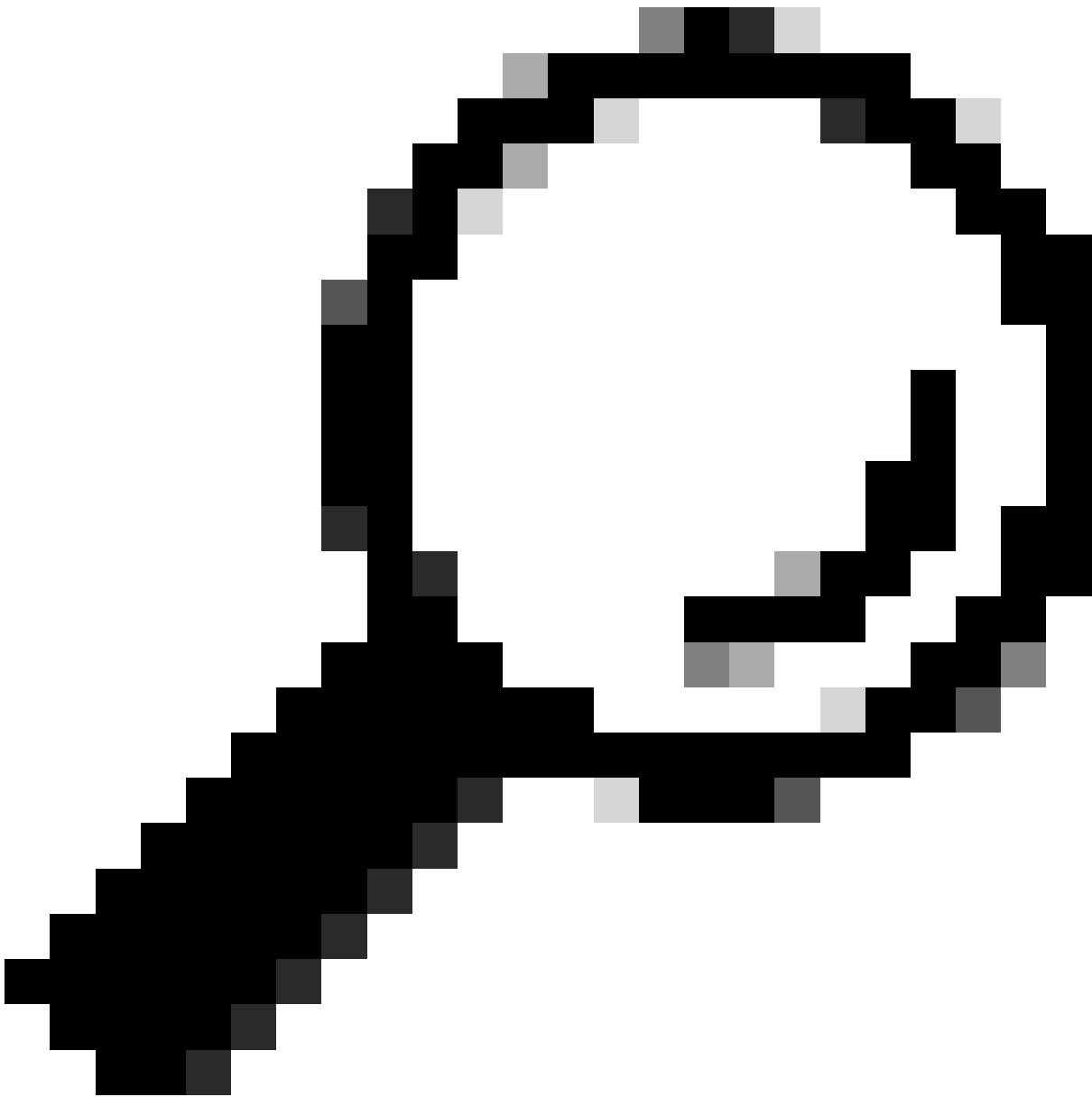
Het DLP-systeem scant het verzoek en retourneert een vonnis naar de webproxy, ofwel blokkeert of controleert (evalueer het verzoek aan de hand van het toegangsbeleid).

Stap 1	Kies Web Security Manager > Preventie van extern gegevensverlies.
Stap 2	Klik op de koppeling onder de kolom Bestemmingen voor de beleidsgroep die u wilt configureren.
Stap 3	Kies onder de sectie Bestemmingsinstellingen bewerken de optie "Bestemmingen definiëren scannen met aangepaste instellingen."
Stap 4	Kies een van de opties in het gedeelte Bestemming om te scannen: <ul style="list-style-type: none"> • Scan geen uploads. Er worden geen uploadverzoeken naar het geconfigureerde DLP-systeem (Data Loss Prevention) voor een scan verzonden. Alle uploadverzoeken worden beoordeeld aan de hand van het toegangsbeleid. • Scan alle uploads. Alle uploadverzoeken worden naar het (de) geconfigureerde DLP-systeem(en) gestuurd om te worden gescand. Het uploadverzoek wordt

	<p>geblokkeerd of beoordeeld aan de hand van het toegangsbeleid; dit is afhankelijk van de uitspraak van het DLP-systeem.</p> <ul style="list-style-type: none">• Scannen uploaden behalve naar aangepaste en externe URL-categorieën. Uploadaanvragen die in specifieke aangepaste URL-categorieën vallen, worden uitgesloten van DLP-scanbeleid. Klik op Aangepaste categorieënlijst bewerken om de URL-categorieën te selecteren die moeten worden gescand.
Stap 5	Veranderingen verzenden en doorvoeren.

URL's voor bypass en doorgifte

U kunt de Secure Web Applicatie in transparante proxy-implementatie configureren om de HTTP- of HTTPS-verzoeken van bepaalde clients of naar bepaalde bestemmingen te omzeilen.



Tip: u kunt passthrough gebruiken voor toepassingen waarvoor verkeer door het apparaat moet worden getransporteerd, zonder dat u wijzigingen of certificaatcontroles van de doelservers hoeft door te voeren

 Waarschuwing: de functie Domain Map werkt in de modus HTTPS Transparant. Deze optie werkt niet in de modus Expliciet en voor HTTP-verkeer.

- De lokale categorie Aangepaste moet worden geconfigureerd om het verkeer deze functie te laten gebruiken.
- Als deze functie is ingeschakeld, wordt de servernaam aangepast of toegewezen volgens de servernaam die in de Domain Map is ingesteld, zelfs als er informatie over de servernaam (SNI) beschikbaar is.

- Deze functie blokkeert geen verkeer op basis van domeinnaam als dat verkeer overeenkomt met de Domeinkaart en corresponderen douanecategorie, decryptie beleid en passthrough actie zijn geconfigureerd.
- Verificatie werkt niet met deze pass-functie. Voor verificatie is decryptie nodig, maar verkeer wordt in dit geval niet gedecrypteerd.
- het verkeer wordt niet bewaakt. U moet UDP-verkeer configureren om niet naar de Web Security Appliance te komen, maar het moet direct via de firewall naar het internet gaan voor toepassingen zoals WhatsApp, Telegram enzovoort.
- WhatsApp, Telegram en Skype werkt in de modus Transparant. Sommige apps zoals WhatsApp werken echter niet in Expliciete modus vanwege beperkingen op de app.

Zorg ervoor dat u een identificatiebeleid hebt gedefinieerd voor de apparaten die doorvoer van verkeer naar specifieke servers vereisen. U moet met name:

- Kies Vrijstellen van verificatie/identificatie.
- Geef de adressen op waarop dit identificatieprofiel van toepassing moet zijn. U kunt IP-adressen, Classless Inter-Domain Routing (CIDR)-blokken en subnetten gebruiken.

Stap 1	HTTPS-proxy inschakelen.
Stap 2	<p>Kies Web Security Manager > Domain Map.</p> <ol style="list-style-type: none"> Kies Domein toevoegen. Voer de domeinnaam of de doelservers in. Kies de volgorde van de prioriteit als er bepaalde domeinen zijn opgegeven. Voer de IP-adressen in. Klik op Verzenden.
Stap 3	<p>Kies Web Security Manager > Aangepaste en externe URL-categorieën.</p> <ol style="list-style-type: none"> Kies Categorie toevoegen. Verstrek deze informatie.

Instellingen	Beschrijving
Categoriennaam	Voer een id in voor deze URL-categorie. Deze naam verschijnt wanneer u URL filter voor beleidsgroepen vormt.
Lijstvolgorde	<p>Specificeer de volgorde van deze categorie in de lijst met aangepaste URL-categorieën. Typ "1" voor de eerste URL-categorie in de lijst.</p> <p>De URL filter engine evalueert een client verzoek aan de aangepaste URL categorieën in de opgegeven volgorde.</p>
Categorietype	Kies lokale aangepaste categorie.
Geavanceerd	<p>U kunt reguliere expressies in deze sectie invoeren om extra sets adressen op te geven.</p> <p>U kunt reguliere expressies gebruiken om meerdere adressen op te geven die overeenkomen met de patronen die u invoert.</p>

c. Verzend en leg de wijzigingen vast.

Stap 4

Kies Web Security Manager > Decryptie Beleid.


- a. Maak een nieuw decryptie beleid.
- b. Kies het identificatieprofiel dat u hebt gemaakt om HTTPS-verkeer voor specifieke toepassingen te omzeilen.
- c. Klik in het paneel Geavanceerd op de koppeling voor URL-categorieën.
- d. Klik in de kolom Toevoegen op om de aangepaste URL-categorie toe te voegen die in stap 3 is gemaakt.
- e. Kies Gereed.
- f. Klik op de pagina Decryptie Beleid op de link voor URL-filtering.
- g. Kies Doorgaan.
- h. Verzend en leg de wijzigingen vast.

(Optioneel) U kunt de % (format specifier) gebruiken om informatie over het

	toegangslogboek te bekijken.
--	------------------------------

Web Proxy-omzeiling configureren voor webaanvragen

Zodra u de Aangepaste URL-categorieën aan de lijst van proxy-omzeilen toevoegt, worden alle IP-adressen en de domeinnamen van de aangepaste URL-categorieën omzeild voor zowel de bron als de bestemming.

Stap 1	Kies Web Security Manager > Instellingen omzeilen.
Stap 2	Klik op Instellingen omzeilen bewerken.
Stap 3	Voer de adressen in waarvoor u de webproxy wilt omzeilen.  Opmerking: wanneer u /0 configureert als een subnetmasker voor een IP in de omzeilingslijst, omzeilt het apparaat al het webverkeer. In dit geval interpreteert het apparaat de configuratie als 0.0.0.0/0.
Stap 4	Kies de Aangepaste URL-categorieën die u wilt toevoegen aan de lijst met proxy-omzeilen.
Stap 5	Verzend en leg uw wijzigingen vast.

 **Waarschuwing:** u kunt de webproxy-omzeilen voor Reguliere expressies niet instellen.

Rapporten

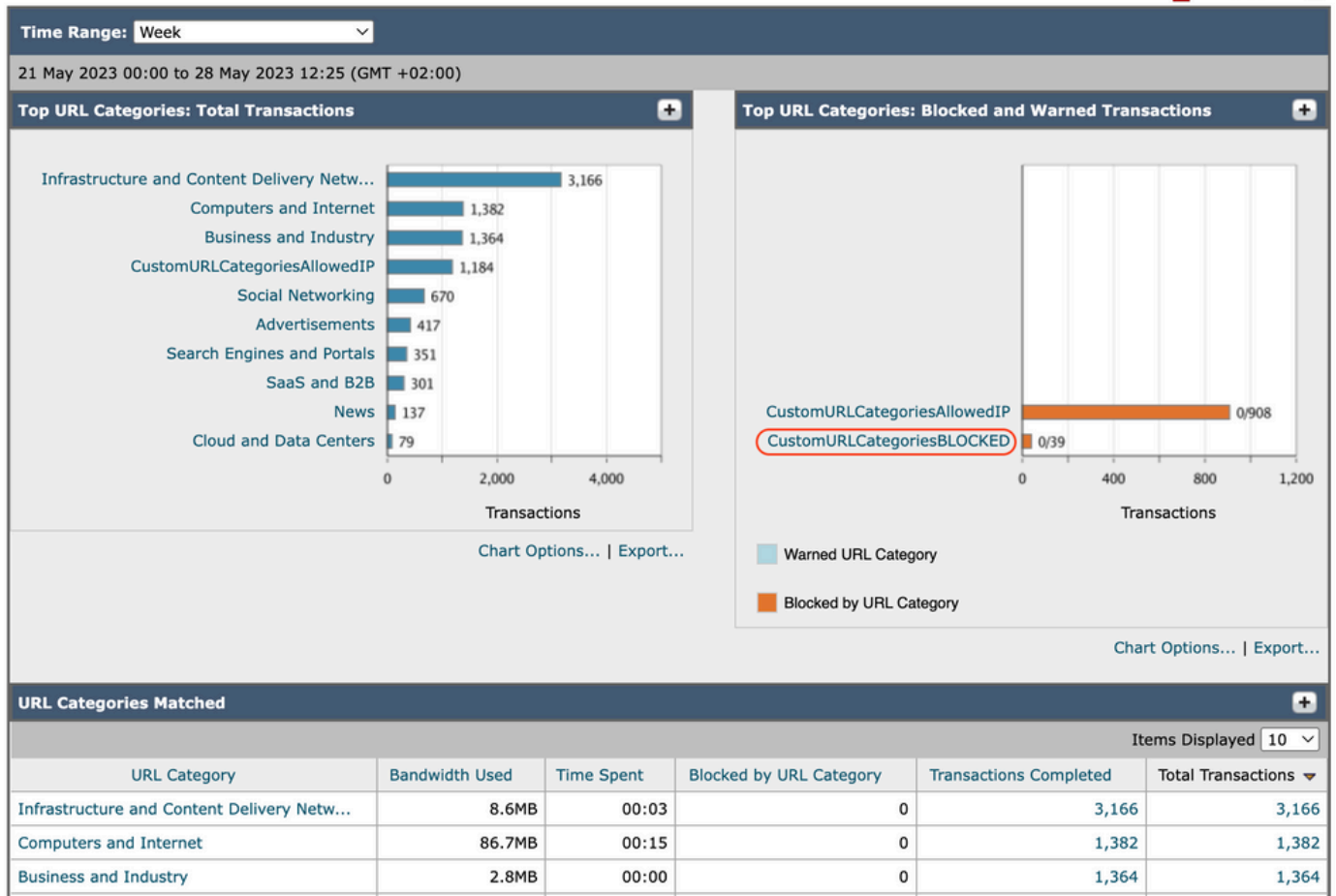
Op de pagina "Rapportage" >> URL-categorieën vindt u een collectieve weergave van URL-statistieken met informatie over overeenkomende URL-categorieën en geblokkeerde URL-categorieën.

Deze pagina toont categorie-specifieke gegevens voor bandbreedtebesparingen en webtransacties.

Deel	Beschrijving
Tijdbereik (vervolgkeuzelijst)	Kies de tijdschaal voor uw rapport.

Deel	Beschrijving
Belangrijkste URL-categorieën op totale transacties	Deze sectie geeft de bovenste URL-categorieën aan die op de site worden bezocht in een grafiekindeling.
Belangrijkste URL-categorieën op geblokkeerde en gewaarschuwde transacties	Een lijst van de hoogste URL die een blok of waarschuwingsactie teweegbracht om per transactie in een grafiekformaat voor te komen.
URL-categorieën gevonden	<p>Toont de regeling van transacties per URL-categorie tijdens de opgegeven tijdschaal, plus de gebruikte bandbreedte en de tijd die in elke categorie wordt doorgebracht.</p> <p>Als het percentage niet-gecategoriseerde URL's hoger is dan 15-20%, overweeg dan deze opties:</p> <ul style="list-style-type: none"> • Voor specifieke gelocaliseerde URL's kunt u aangepaste URL-categorieën maken en deze op specifieke gebruikers of groepsbeleid toepassen. • U kunt ongecategoriseerde en verkeerd geclassificeerde en URLs aan Cisco voor evaluatie en gegevensbestandupdate melden. • Controleer of Web Reputation Filter en Anti-Malware Filter zijn ingeschakeld.

URL-Categories

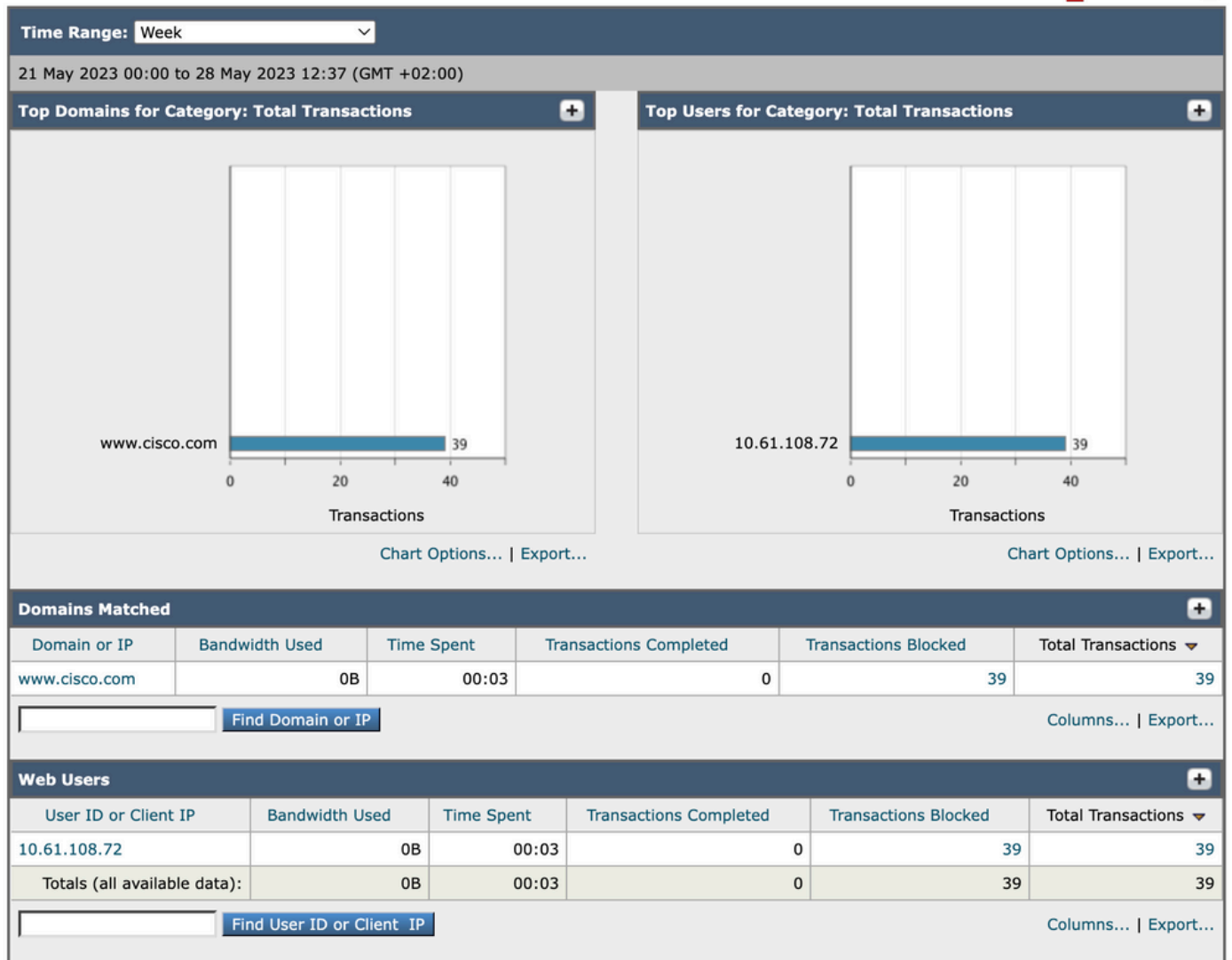


Categorieverslag voor afbeelding/URL

U kunt op elke categorienaam klikken om meer details met betrekking tot die categorie te bekijken, zoals de lijst met overeenkomende domeinen of gebruikers.

URL Categories > CustomURLCategoriesBLOCKED

Printable PDF 



Afbeelding - Gedetailleerde rapportpagina

De set van vooraf gedefinieerde URL-categorieën kan periodiek automatisch worden bijgewerkt op uw Web security applicatie .

Wanneer deze updates zich voordoen, blijven oude categorienamen in rapporten verschijnen totdat de gegevens die gekoppeld zijn aan de oudere categorieën te oud zijn om in rapporten te worden opgenomen.

Rapportgegevens die zijn gegenereerd nadat een URL-categorieupdate de nieuwe categorieën gebruikt, zodat u zowel oude als nieuwe categorieën in hetzelfde rapport kunt zien.

In URL-statistieken op de pagina URL-categorieën van rapporten is het belangrijk om te begrijpen hoe deze gegevens geïnterpreteerd moeten worden:

Gegevenstype	Beschrijving
URL-filtering overgeslagen	Vertegenwoordigt beleid, poort en beheerder geblokkeerde gebruikersagent die voor URL-filtering optreedt.

Niet-gecategoriseerde URL

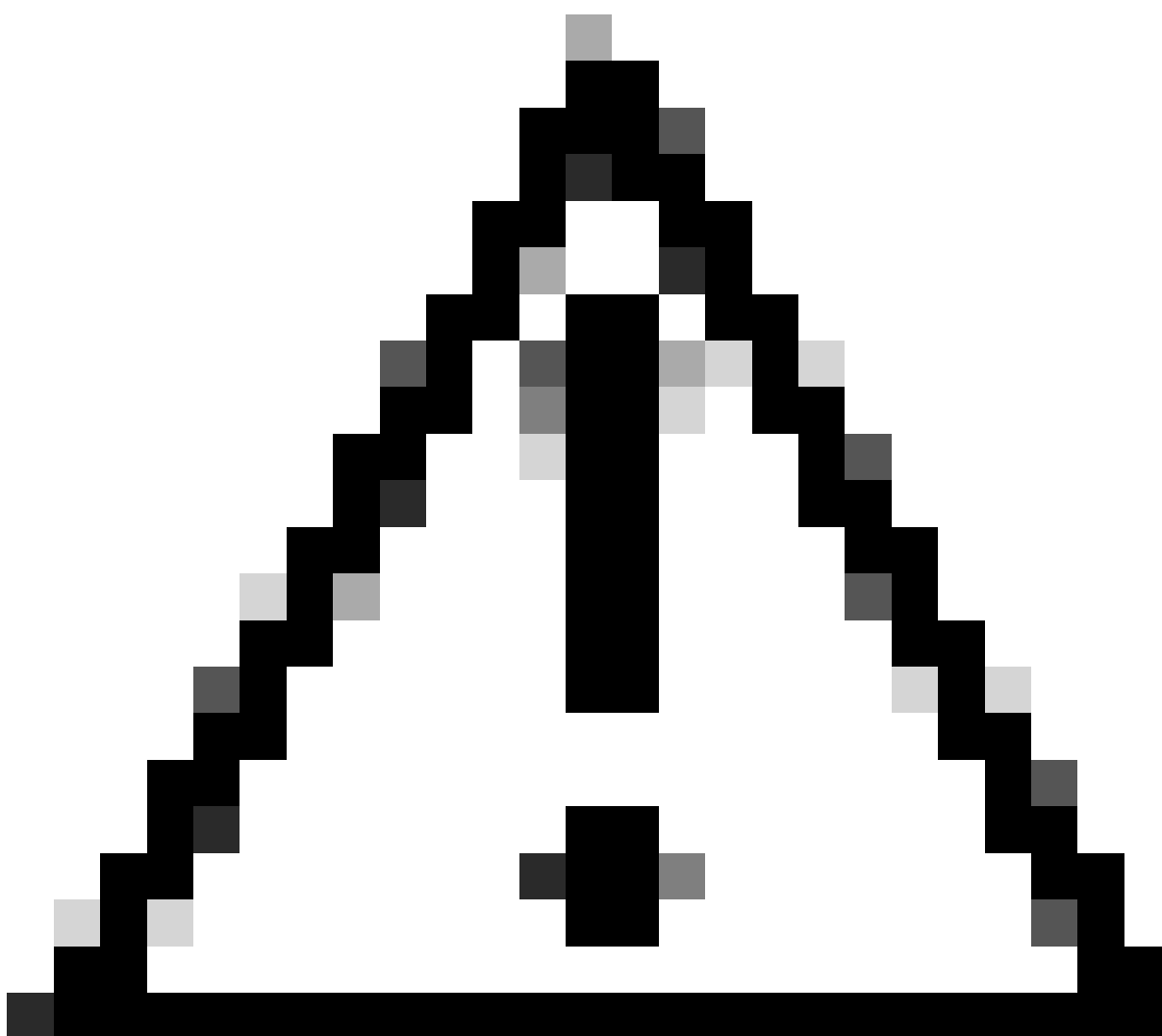
Vertegenwoordigt alle transacties waarvoor de URL-filtreermotor is gevraagd, maar er is geen categorie gekoppeld.

Aangepaste URL-categorieën in het toegangslogboek bekijken

De Secure Web Applicatie gebruikt de eerste vier tekens van aangepaste URL-categorienamen voorafgegaan door "c_" in de toegangslogbestanden.


In dit voorbeeld is de categorienaam CustomURLCategoriesBLOCKED en in de toegangslijsten kunt u C_Cust zien:

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



Waarschuwing: overweeg de aangepaste URL categorie naam als u Sawmill gebruikt om

de toegangslogboeken te parseren. Als de eerste vier tekens van de aangepaste URL-categorie een spatie bevatten, kan Zagerij de ingang van het toegangslogboek niet goed parseren. Gebruik in plaats daarvan alleen ondersteunde tekens in de eerste vier tekens.

 Tip: Als u de volledige naam van een aangepaste URL-categorie wilt opnemen in de toegangslogbestanden, voegt u de specifier %XF-indeling toe aan de toegangslogbestanden.

Wanneer een webtoegangsbeleidsgroep een aangepaste URL-categorie heeft die is ingesteld op Monitor en een andere component (zoals de webreputatiefilters of de DVS-engine (Different Verdicts Scanning)) het definitieve besluit neemt om een verzoek voor een URL in de aangepaste URL-categorie toe te staan of te blokkeren, dan toont het toegangslogboek voor het verzoek de vooraf gedefinieerde URL-categorie in plaats van de aangepaste URL-categorie.

Voor meer informatie over het configureren van aangepaste velden in toegangslogbestanden gaat u naar: [Prestatieparameter configureren in toegangslogbestanden - Cisco](#)

Problemen oplossen

Categorie mismatched

Van de toegangslogboeken kunt u zien het verzoek tot welke Aangepaste URL Categorie behoort, als de selectie niet zoals verwacht is:

- Als de aanvraag is gecategoriseerd naar andere aangepaste URL-categorieën, controleer dan op dubbele URL of een overeenkomende reguliere expressie in andere categorieën of verplaats de aangepaste URL-categorie naar boven en test deze opnieuw. Het is beter om de aangepaste URL-categorie zorgvuldig te inspecteren.

- Als het verzoek is gecategoriseerd naar vooraf gedefinieerde categorieën, controleer de voorwaarden in de bestaande aangepaste URL-categorie, als alle overeenkomsten, probeer om het IP-adres toe te voegen en test of zorg ervoor dat de typo en correcte reguliere expressie wordt gebruikt, als er een.

De vooraf bepaalde categorieën zijn niet bijgewerkt

Als de vooraf gedefinieerde categorieën niet bijgewerkt zijn, of in de toegangslijsten die u ziet "vergissen" in de URL-categorie sectie, zorg ervoor dat TLSv1.2 is ingeschakeld voor Updater.

Om de Updater SSL-configuratie te wijzigen, gebruikt u deze stappen van GUI:

Stap 1. Kies SSL-configuratie vanuit systeembeheer

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

Configuratie van image-ssl

Stap 2. Kies Instellingen bewerken.

Stap 3. Kies in het gedeelte Service bijwerken TLSv1.2

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:NULL: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

Afbeelding - Service TLSv1.2 bijwerken

Stap 4. Wijzigingen verzenden en vastleggen

Om de Updater SSL configuratie te veranderen, gebruik deze stappen van CLI:

Stap 1. Vanuit CLI voert u sslconfig uit

Stap 2. Typ de versie en druk op ENTER

Stap 3. Updater kiezen

Stap 4. Kies TLSv1.2

Stap 5. Druk op ENTER om de wizard te verlaten

Stap 6. Verbind de veranderingen.

```
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 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.

Referentie

[Richtlijnen voor beste praktijken van Cisco Web Security Applicatie - Cisco](#)

[BRKSEC-3303 \(ciscolive\)](#)

[Gebbruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Applicatie - GD \(Algemene implementatie\) - Verbinden, installeren en configureren \[Cisco Secure Web Applicatie\] - Cisco](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.