

Aangepaste URL-rubrieken definiëren in WSA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[URL's toestaan](#)

[Een nieuwe aangepaste URL maken](#)

[Het algemene toegangsbeleid bewerken](#)

[URL's blokkeren](#)

[Een nieuwe aangepaste URL maken](#)

[Het algemene toegangsbeleid bewerken](#)

Inleiding

In dit document wordt beschreven hoe u aangepaste URL-categorieën kunt definiëren die werken in Web Security Appliance (WSA).

Bijgedragen door Shikha Grover en bewerkt door Yeraldin Sanchez, Cisco TAC Engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beginnersniveau van Cisco Web Security Appliance

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.

Achtergrondinformatie

De categorie waarin een URL valt, wordt bepaald door een database met filtercategorieën. Het

Web Security-apparaat verzamelt informatie en onderhoudt een afzonderlijke database voor elke URL-filterengine. De filtercategorieën databases ontvangen periodiek updates van de Cisco-updateserver en worden onderhouden door Cisco TALOS. Talos, de Security Intelligence and Research Group van Cisco, houdt voortdurend een breed scala aan kenmerken bij om conclusies over een bepaalde host te evalueren.

Er kunnen situaties zijn waarin u een URL / domein / IP-adres anders wilt classificeren en een aangepaste lokale classificatie aan uw vak wilt aanpassen. U kunt dit bereiken met aangepaste URL-rubrieken.

Wanneer de URL-filterengine een URL-categorie koppelt aan de URL in een clientverzoek, evalueert deze eerst de URL aan de hand van de aangepaste URL-categorieën in de beleidsgroep. Als de URL in de aanvraag niet overeenkomt met een bijgeleverde aangepaste categorie, vergelijkt de URL-filterengine deze met de vooraf gedefinieerde URL-categorieën.

Configureren

URL's toestaan

Als u de website vertrouwt, kunt u dit toestaan met het volgende proces.

Een nieuwe aangepaste URL maken

1. Maak een nieuwe aangepaste URL-rubriek, navigeer naar GUI > Web Security Manager > Aangepaste URL-rubrieken > Aangepaste rubrieknaam toevoegen: Toegestane URL's.
2. Voeg de sites toe die u wilt beheren in de sectie sites (company.com, .company.com).

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:

Comments: (?)

List Order:

Category Type: Local Custom Category

Sites: (?)

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Regular Expressions: (?)

Enter one regular expression per line.

- 3.
4. Houd er rekening mee dat "domain.com" alleen overeenkomt met "domain.com", niet met www.domain.com of "host.domain.com". Om een site en alle subdomeinen toe te staan, heeft deze twee vermeldingen nodig onder de sectie "sites": ". domain.com, domain.com".
5. Klik op Verzenden.

Het algemene toegangsbeleid bewerken

1. Open Webbeveiligingsbeheer > Toegangsbeleid > Algemeen beleid > URL-filtering.
2. Klik op Aangepaste rubrieken selecteren.
3. Klik op de vervolgkeuzelijst Toegestane URL's, kies Opnemen in beleid en klik op Toepassen.
4. Plaats een vinkje in het vak Toestaan.
5. Klik op Verzenden en Wijzigingen vastleggen.

Access Policies: URL Filtering: Global Policy

Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-based	Time-based
Allowed URLs	Custom (LOCAL)	Select all	Select all	Select all	Select all	Select all		

URL's blokkeren

Als u de website niet vertrouwt, kunt u deze blokkeren met het volgende proces.

Een nieuwe aangepaste URL maken

1. Maak een nieuwe aangepaste URL-categorie, navigeer naar GUI > Web Security Manager > Aangepaste URL-rubrieken > Aangepaste rubrieknaam toevoegen: geblokkeerde URL's.
2. Voeg de sites toe die u wilt beheer in de sectie sites (company.com, .company.com).

Custom and External URL Categories: Edit Category

Category Name:

Comments:

List Order:

Category Type: Local Custom Category

Sites:

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Regular Expressions:

Enter one regular expression per line.

3. Houd er rekening mee dat "domain.com" alleen overeenkomt met "domain.com", niet met www.domain.com of "host.domain.com". Om een site en alle subdomeinen te blokkeren, heeft het twee vermeldingen nodig onder de sectie "sites": ". domain.com, domain.com".
4. Klik op Verzenden.

Het algemene toegangsbeleid bewerken

1. Open Webbeveiligingsbeheer > Toegangsbeleid > Algemeen beleid > URL-filtering.

2. Klik op Aangepaste rubrieken selecteren....
3. Klik op de vervolgkeuzelijst Geblokkeerde URL's, kies Opnemen in beleid en klik op Toepassen.
4. Plaats een vinkje in het vak voor Blokkeren.
5. Klik op Verzenden en Wijzigingen vastleggen.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering		Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.								
Category	Category Type	Select all	Select all	Select all	Select all	Select all		
Blocked URLs	Custom (Local)	☒						
Select Custom Categories...								

 **Opmerking:** de bovenstaande wijzigingen kunnen worden aangebracht in elk toegangsbeleid en niet alleen in het algemene beleid. Dezelfde procedure kan worden toegepast op decryptie beleid.

Raadpleeg deze [handleiding](#) voor een breed ingezette use case.

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.