Web Reputation score (WBRS) en Web Category Engine Vaak gestelde vragen (FAQ)

Inhoud

Web Reputation score (WBRS) en Web Category Engine stelden vragen (FAQ) vaak.

Dit artikel beschrijft de meest frequent gestelde vragen op Web Reputation Score (WBRS) en Categorieoptie met de Cisco Web Security Appliance (WSA).

Wat betekent een Web Reputation Score?

Web Reputation Filters wijzen een Web-Based Reputation Score (WBRS) aan een URL toe om de waarschijnlijkheid te bepalen dat deze op URL gebaseerde malware bevat. Web security applicatie gebruikt platforminfcaties om malware aanvallen te identificeren en te stoppen voordat ze zich voordoen. U kunt Web Reputation Filters met Access, Decryptie, en Cisco gegevensveiligheidsbeleid gebruiken.

Wat betekent een webcategorisering?

De internetwebsites zijn categorieën op basis van het gedrag en het doel van deze websites, om het voor de beheerders van de volmachten gemakkelijker te maken, hebben we elke URL van de website toegevoegd aan een vooraf gedefinieerde categorie, waar deze kan worden geïdentificeerd voor veiligheids- en rapportagedoeleinden. websites die niet tot een van de vooraf gedefinieerde categorieën behoren, worden niet-gecategoriseerde websites genoemd, die kunnen worden veroorzaakt door nieuwe websites en een gebrek aan voldoende gegevens/verkeer om de categorie ervan te bepalen. en dit verandert mettertijd .

Hoe vind je de reputatie score in toegangsdocumenten?

Elk verzoek dat u via de Cisco Web Security Appliance (WSA) maakt, moet een Web-Based Reputation Score (WBRS) score en URL categorie aan het programma hebben bevestigd. en een van de manieren om het te bekijken is via de toeganglogs , is een voorbeeld : de Web-Based Reputation Score (WBRS) score is (-1.4) en de URL-categorie is: Computers en internet.

Tekstreferentie voor de bovenstaande screenshot.

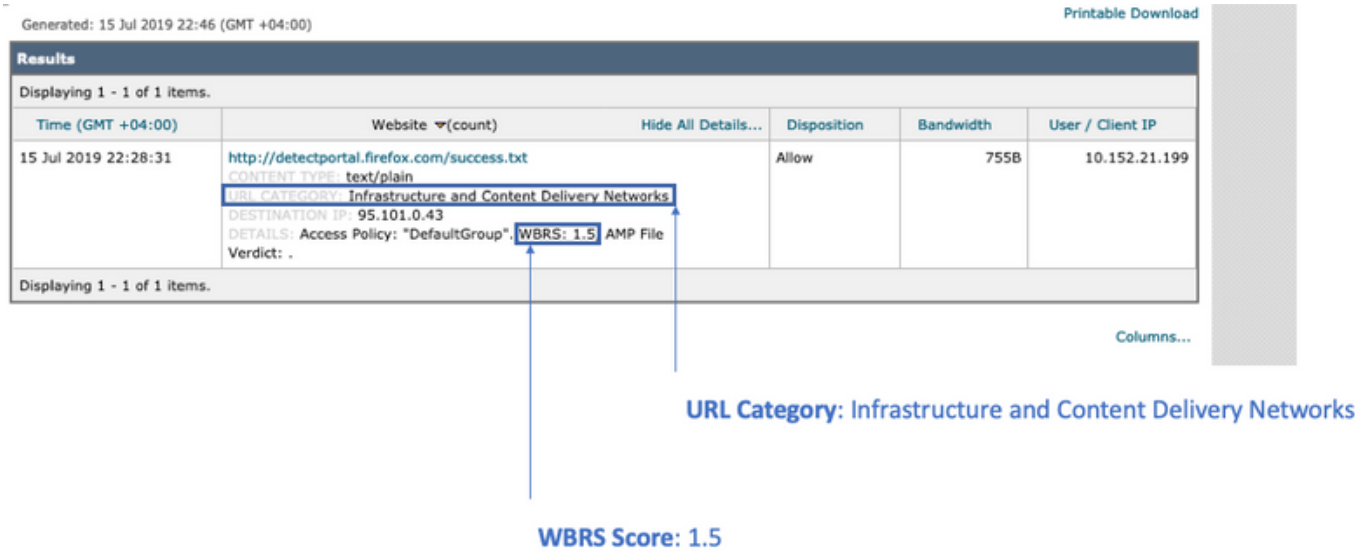
1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE ,0,"-",0,0,0,-,"-",-,-,-,"-","-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-","-",-,-,"-","-",-,-,"-",-> -

Opmerkingen:

- Access logs kunnen worden bekeken vanaf Opdracht Line Interface (CLI) of gedownload door de bestandsoverdrachtmethode (FTP) op de beheerinterface IP aan te sluiten. (Controleer of FTP op de interface is ingeschakeld).
- Volledige lijst van categorieën Afkorting: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01001.html#con_1208638

Hoe vind je de reputatie score in mijn verslagen?

1. Navigeer naar Cisco Web Security Appliance (WSA) **GUI** -> **Rapportage** -> **Web Tracking**.
2. Zoek het **domein** dat u zoekt.
3. Klik in de pagina **Resultaten** op de gewenste link en meer details worden weergegeven zoals hieronder.



Waar controleer je de Web-Based Reputation Score (WBRS) updates?

Web-Based Reputation Score (WBRS) updates zijn te vinden in de update_logs en u kunt deze bestanden downloaden via File Transfer Protocol (FTP) en inloggen op de beheerinterface. of via Opdrachtlijn Interface (CLI).

U kunt Logs als volgt weergeven met behulp van terminal:

1. Open **terminal**.
2. Typ de opdracht **staart**.
3. Kies het **lognummer** (dit varieert afhankelijk van de versie en het aantal geconfigureerde logbestanden).
4. De logbestanden worden weergegeven.

```
WSA.local (SERVICE)> tail

Currently configured logs:
1. "xx.xx.xx.xx" Type: "Configuration Logs" Retrieval: FTP Push - Host
xx.xx.xx.xx
2. "Splunk" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Push - Host xx.xx.xx.xx
4. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
5. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
....
43. "uds_logs" Type: "UDS Logs" Retrieval: FTP Poll
44. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP
Poll
Enter the number of the log you wish to tail.
[]> 44

Press Ctrl-C to stop scrolling, then `q` to quit.
```

```
Mon Jul 15 19:24:04 2019 Info: mcafee updating the client manifest
Mon Jul 15 19:24:04 2019 Info: mcafee update completed
Mon Jul 15 19:24:04 2019 Info: mcafee waiting for new updates
Mon Jul 15 19:36:43 2019 Info: wbrs preserving wbrs for upgrades
Mon Jul 15 19:36:43 2019 Info: wbrs done with wbrs update
Mon Jul 15 19:36:43 2019 Info: wbrs verifying applied files
Mon Jul 15 19:36:58 2019 Info: wbrs Starting heath monitoring
Mon Jul 15 19:36:58 2019 Info: wbrs Initiating health check
Mon Jul 15 19:36:59 2019 Info: wbrs Healthy
Mon Jul 15 19:37:14 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:15 2019 Info: wbrs Healthy
Mon Jul 15 19:37:30 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:31 2019 Info: wbrs Healthy
Mon Jul 15 19:37:46 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:47 2019 Info: wbrs Healthy
Mon Jul 15 19:38:02 2019 Info: wbrs updating the client manifest
Mon Jul 15 19:38:02 2019 Info: wbrs update completed
Mon Jul 15 19:38:03 2019 Info: wbrs waiting for new updates
Mon Jul 15 20:30:23 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 20:30:24 2019 Info: Scheduled next release notification fetch to occur at Mon Jul 15
23:30:24 2019
Mon Jul 15 23:30:24 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 23:30:25 2019 Info: Scheduled next release notification fetch to occur at Tue Jul 16
02:30:25 2019
```

Hoe verifieert u of u connectiviteit hebt op Web-Based Reputation Score (WBRS) updates van servers?

Om ervoor te zorgen dat uw Cisco Web Security Appliance (WSA) de nieuwe updates kan krijgen. controleer of u de connectiviteit met de servers van Cisco update op de volgende poorten 80 en 443 van het Transmission Control Protocol (TCP) hebt:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.

wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

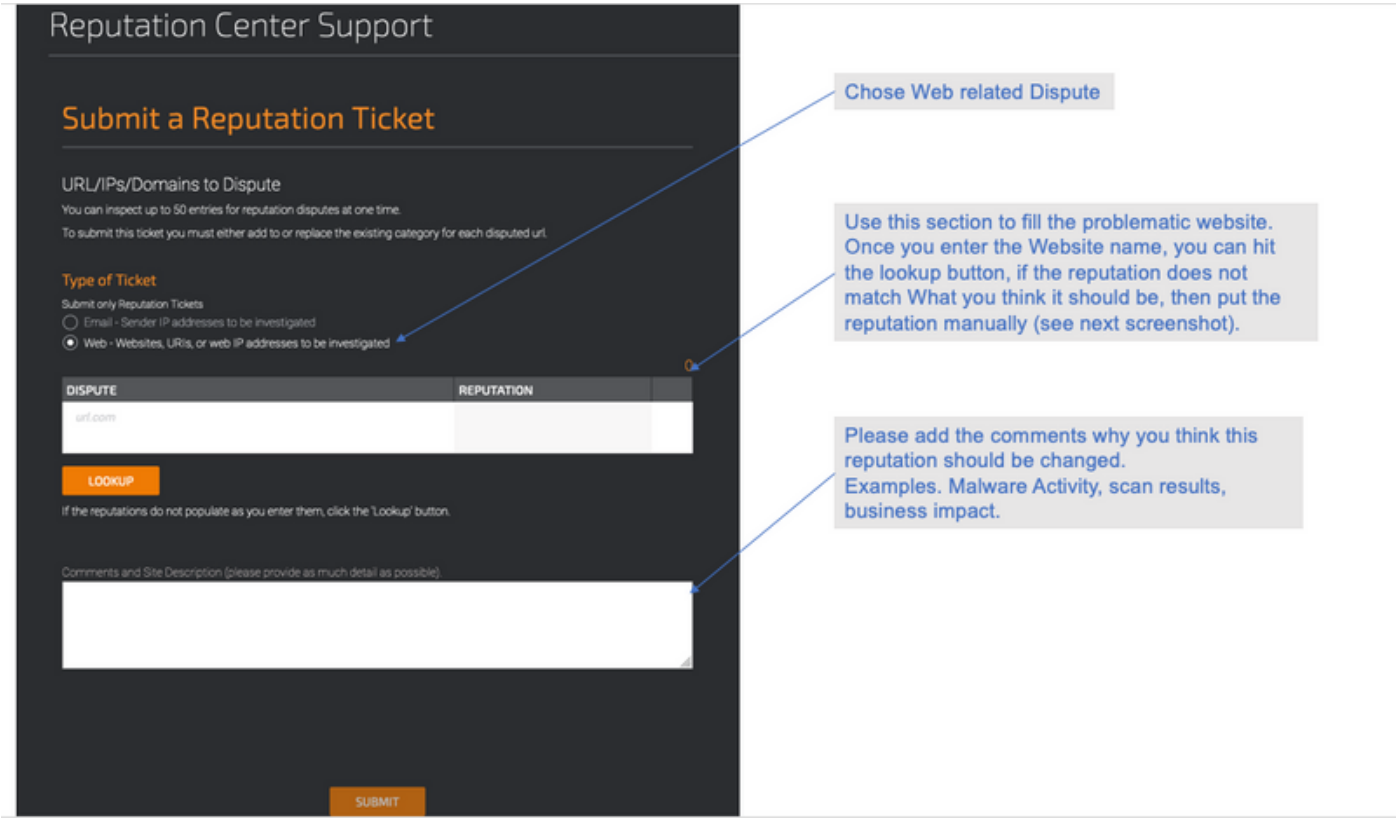
> Opmerking: Als u een stroomopwaartse proxy hebt, voer dan de bovenstaande tests uit via uw stroomopwaartse proxy.

Hoe voert u een geschil in voor webcategorisering?

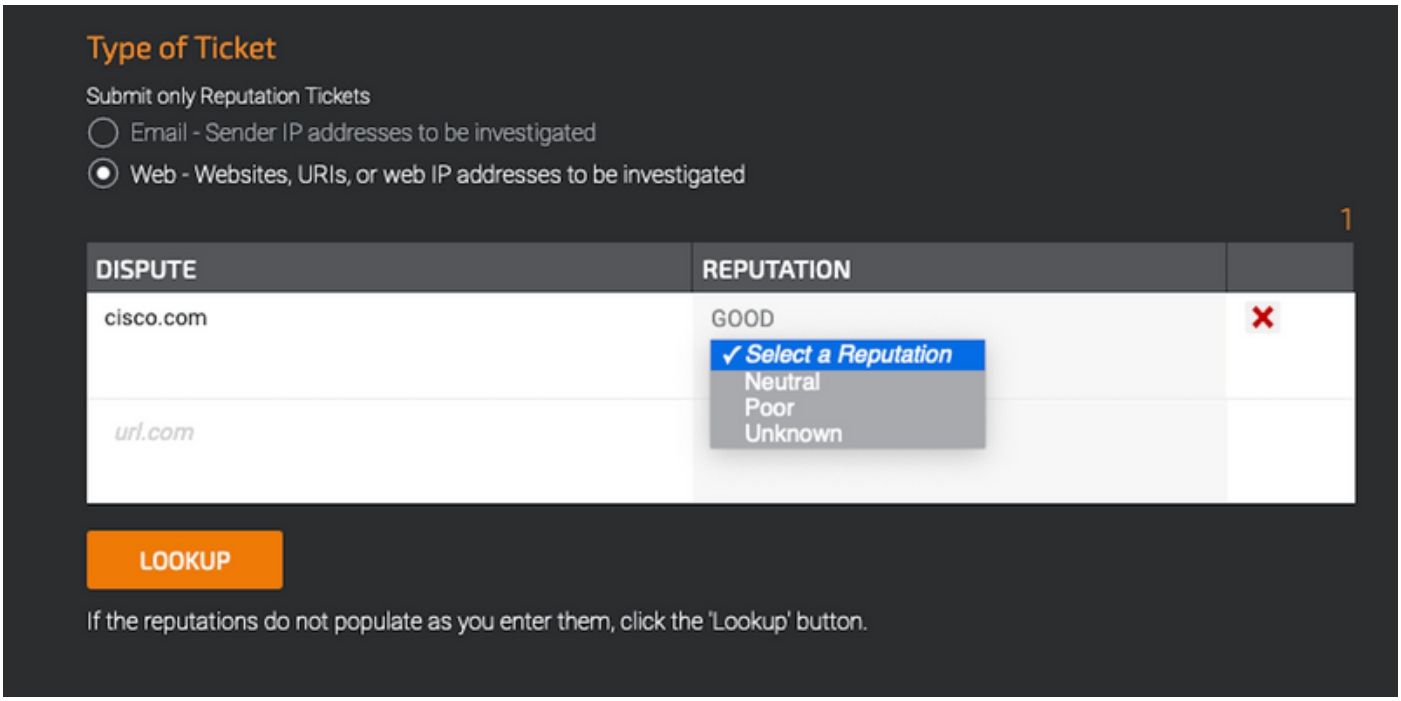
Na het controleren dat zowel Cisco Web Security Appliance (WSA) als Cisco TALOS dezelfde reputatiescore hebben maar u nog steeds denkt dat dit geen geldig resultaat is, moet dit worden vastgesteld door een geschil met Cisco TALOS-team te verzenden.

U kunt dit doen via de volgende link: https://talosintelligence.com/reputation_center/support

Om het **geschil** in **te dienen**, volgt u de onderstaande instructies.



Resultaten nadat u Lookup hebt ingedrukt en de optie om de score handmatig te wijzigen.



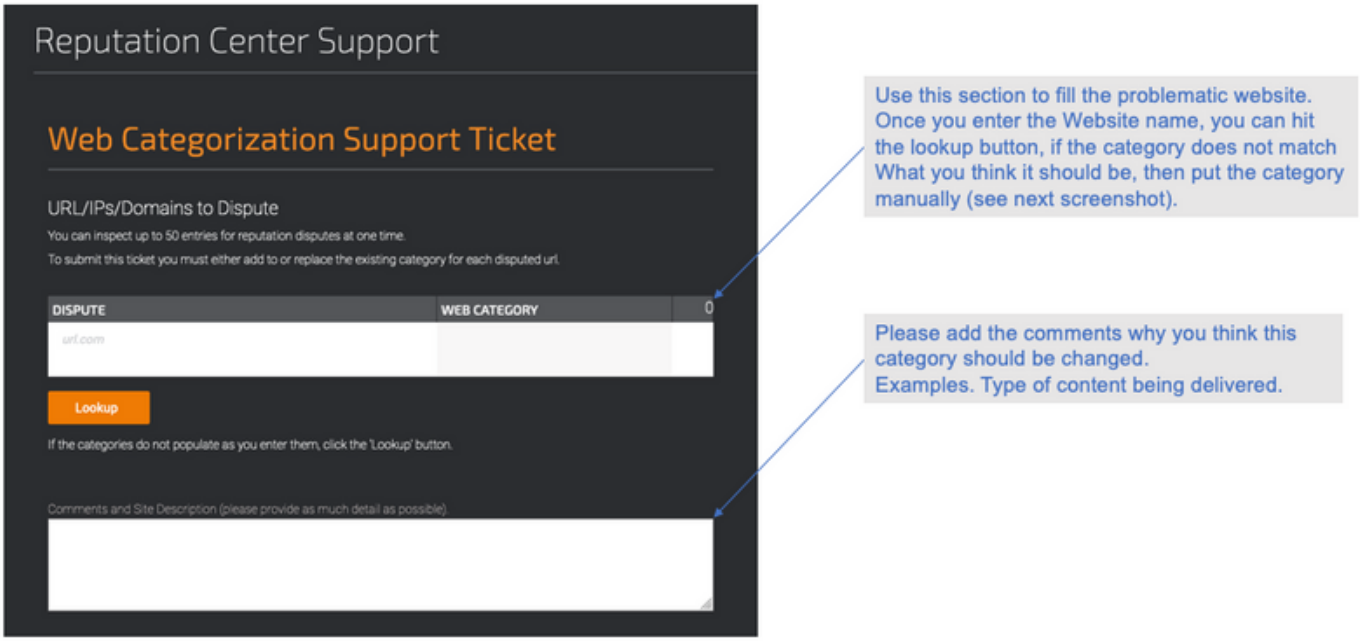
Opmerking: CISCO TALOS-inzendingen kunnen enige tijd in beslag nemen om gereflecteerd te worden in een database als de kwestie dringend is, kunt u altijd een **WHITELIST** of **BLOCKLIST** maken, als tijdelijke oplossing voor de kwestie vanaf Cisco-backend. om dat te doen, kunt u deze sectie controleren (Hoe werkt Whitelist of BlackList URL).

Hoe bevecht je een geschil voor Web Reputation score?

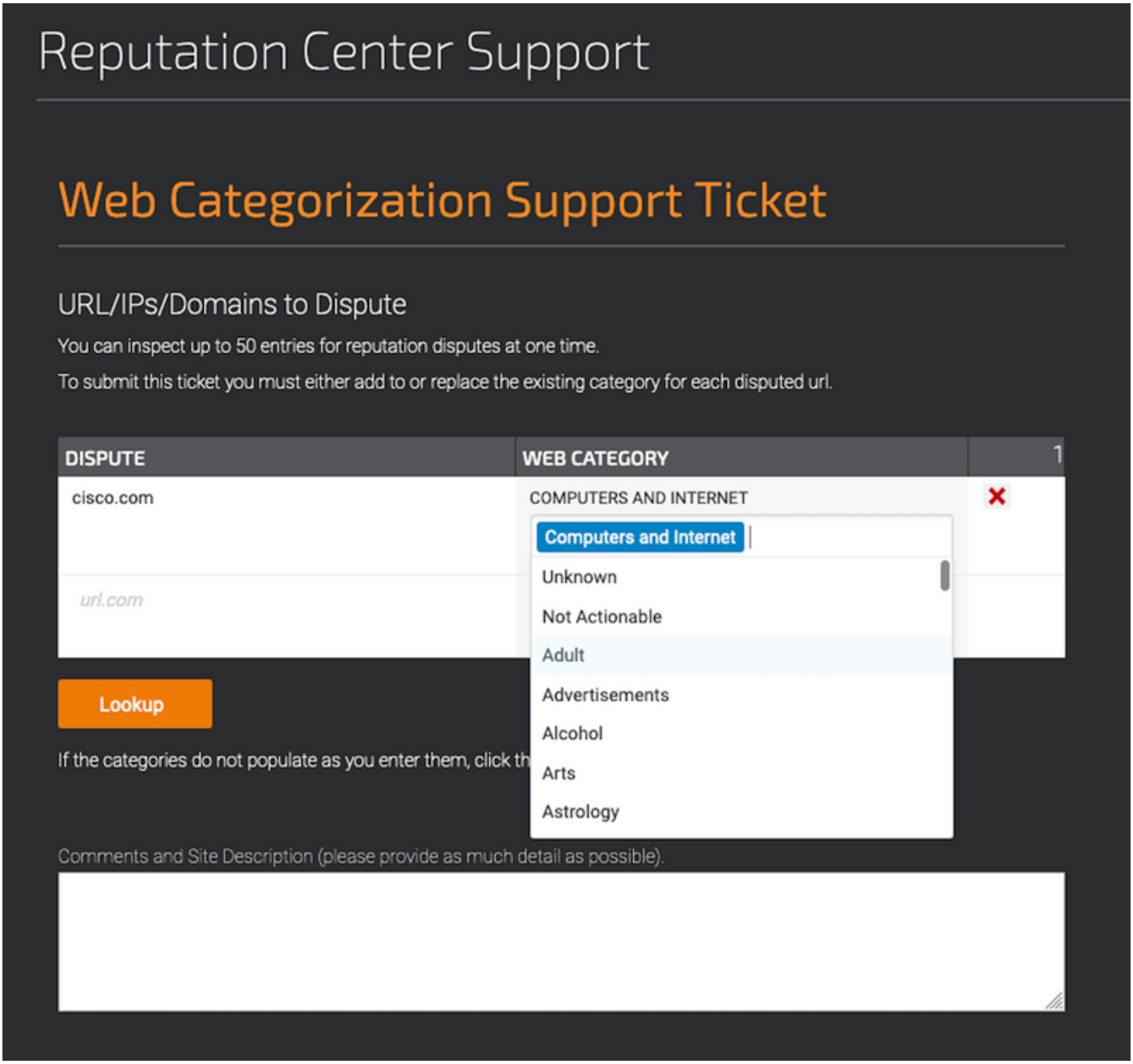
Na het controleren dat zowel Cisco Web Security Appliance (WSA) als Cisco TALOS dezelfde categorieën hebben maar u nog steeds denkt dat dit geen geldig resultaat is, moet dit worden vastgesteld door een geschil met Cisco TALOS-team te verzenden.

Ga naar de pagina voor categorisering in TALOS:
https://talosintelligence.com/reputation_center/support#categorization

Om het **geschil** in **te dienen**, volgt u de onderstaande instructies.



Als u de categorie wilt bijwerken, kiest u in het **vervolgkeuzemenu** wat u vindt dat de inhoud beter op de website past, en volgt u de commentaar-richtlijnen.



Er is een geschil ingediend maar de score of categorie wordt niet bijgewerkt op Cisco Web Security Appliance (WSA) of Cisco TALOS.

Heeft u een case ingediend bij Cisco TALOS en wordt de reputatie/score niet binnen 3-4 dagen bijgewerkt. U kunt uw updates controleren en ervoor zorgen dat u bereikbaarheid hebt aan de server van Cisco update. als al deze stappen ok waren, dan kunt u doorgaan en een ticket openen met Cisco TAC en Cisco Engineer helpt u bij het volgen met Cisco TALOS-team.

> Opmerking: U kunt het WHITELIST/BLOCKLIST-werk toepassen om de gewenste actie toe te passen tot de categorie/reputatie wordt bijgewerkt vanaf Cisco TALOS-team.

Cisco web security applicatie (WSA) verschillende resultaten laten zien dan Cisco TALOS, hoe deze te repareren?

Database kan verouderd zijn op Cisco Web Security Appliance (WSA) vanwege meerdere redenen, voornamelijk communicatie met onze updates servers, volgt deze stappen om te controleren of u juiste update servers en connectiviteit hebt.

1. Controleer dat u de connectiviteit voor de servers van Cisco update op poort 80 en 443 hebt:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.

wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

2. Als u een stroomopwaartse proxy hebt, zorg er dan voor dat de stroomopwaartse proxy ervoor zorgt dat u de bovenstaande tests uitvoert via uw stroomopwaartse proxy.

3. Als de connectiviteit fijn is en u nog steeds het verschil ziet, forceer dan de updates handmatig: **updates** van de CLI, of van **GUI->Security services -> Malware Protection -> updates hieronder**.

Wacht een paar minuten en als dat niet werkt, controleer dan de volgende stap.

4. Op dit moment moet u de update_logs controleren: open **terminal: CLI->tail-> (kies het aantal logbestanden update_logs.)** hierdoor worden de update-logbestanden alleen de nieuwe regels weergegeven.

Loglijnen moeten starten met deze regel "**Ontvangen afstandsbediening om een handmatige update aan te geven**":

```
Mon Jul 15 19:14:12 2019 Info: Received remote command to signal a manual
update
Mon Jul 15 19:14:12 2019 Info: Starting manual update
Mon Jul 15 19:14:12 2019 Info: Acquired server manifest, starting update 342
Mon Jul 15 19:14:12 2019 Info: wbrs beginning download of remote file
"http://updates.ironport.com/wbrs/3.0.0/ip/default/1563201291.inc"
Mon Jul 15 19:14:12 2019 Info: wbrs released download lock
Mon Jul 15 19:14:13 2019 Info: wbrs successfully downloaded file
"wbrs/3.0.0/ip/default/1563201291.inc"
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs applying component updates
Mon Jul 15 19:14:13 2019 Info: Server manifest specified an update for mcafee
Mon Jul 15 19:14:13 2019 Info: mcafee was signalled to start a new update
Mon Jul 15 19:14:13 2019 Info: mcafee processing files from the server manifest
Mon Jul 15 19:14:13 2019 Info: mcafee started downloading files
Mon Jul 15 19:14:13 2019 Info: mcafee waiting on download lock
```

5. Controleer op '**Kritisch/Waarschuwing**'-berichten en de update logbestanden zijn zeer menselijke leesbare fouten en zal u naar alle waarschijnlijkheid begeleiden waar het probleem is.

6. Als er geen antwoord is geweest, kunt u verdergaan en een ticket met Cisco-ondersteuning openen met de resultaten van de bovengenoemde stappen, en ze zullen met plezier helpen.

Hoe worden de scores voor de Web Reputation berekend?

Enkele parameters die in overweging worden genomen bij het toewijzen van een score aan een specifieke website:

- URL-categorisatiegegevens
- Aanwezigheid van de downloadbare code
- Aanwezigheid van lange, verduisterde Gebruiksrechtovereenkomst (EULA's)
- Totale omvang en volumemutaties
- Informatie over de netwerkeigenaar
- Historie van een URL
- Leeftijd van een URL
- Aanwezigheid in alle bloklijsten
- Aanwezigheid op elke toegelaten lijst
- URL-typen van populaire domeinen
- Domain Registrar-informatie
- IP-adresinformatie

Wat is de score voor elk van de reputatiecategorieën (goed, neutraal, arm)?

Web reputatie en bijbehorende acties:

Toegangsbeleid:

kern	Handeling	Beschrijving	Voorbeeld
-10 t/m -6,0 (Arm)	blokkeren	Slechte plek. Het verzoek is geblokkeerd, en geen andere malware scans gebeurt.	• URL downloads zonder informatie. • toestemming van de gebruiker. • Plotselinge piek in URL-volume. • URL is een type van een populair domein.
-5,9 t/m 5,9 (Neutraal)	Scannen	Onbepaalde plaats. Aanvraag is: naar de DVS-motor voor verder scannen van malware. Het DVS-motor scant het verzoek en de inhoud van de serverreactie.	• Recent gemaakte URL die een • dynamisch IP-adres en bevat • downloadbare inhoud. • IP-adres van de netwerkeigenaar dat een • positieve Web Reputation Score.
6,0 t/m 10,0 (goed)	toestaan	Goede site. Aanvraag is toegestaan. Geen malware scan vereist.	• URL bevat geen downloadbare inhoud. • Realiseerbaar, hoog volume domein met lang geschiedenis. • Domain aanwezig op meerdere allow lijsten. • Geen links naar URL's met een slechte reputa

Decryptie beleid:

kern	Handeling	Beschrijving
-10 t/m -9,0	druppel	Slechte plek. Het verzoek wordt ingetrokken zonder kennisgeving aan de

(Arm)		eindgebruiker. Gebruik deze instelling is voorzichtig .
-8,9 t/m 5,9 (Neutraal)	decrypteren	Onbepaalde plaats. Aanvraag is toegestaan, maar de verbinding wordt gedecrypteerd en toegangsbeleid wordt toegepast op het ontsleutelde verkeer.
6,0 t/m 10,0 (goed)	Doorlopen	Goede site. Aanvraag wordt doorgegeven zonder inspectie of decryptie.

Cisco-beleid voor gegevensbeveiliging:

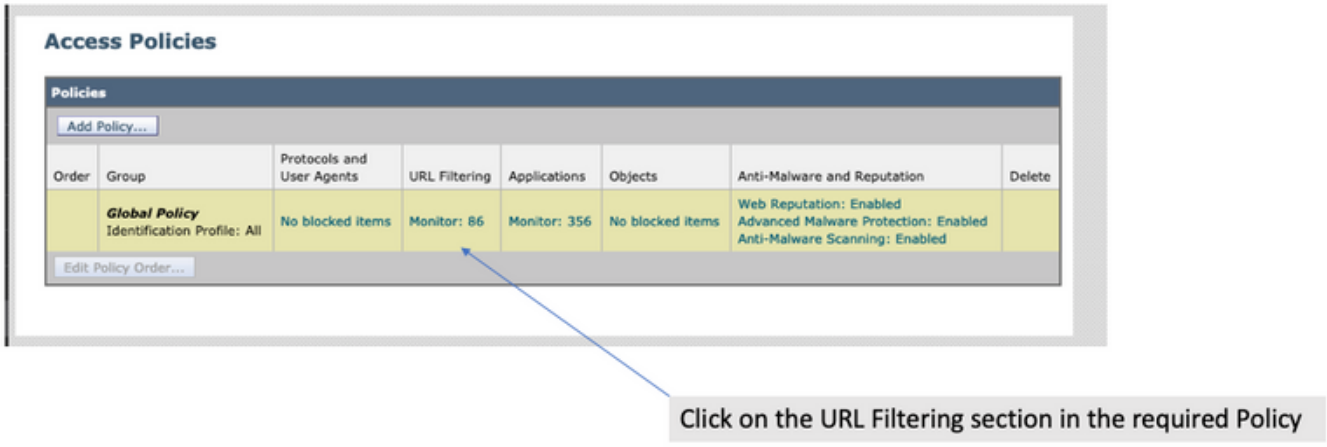
kern	**Handeling**	**Beschrijving**
-10 t/m -6,0 (Arm)	blokkeren	Slechte plek. De transactie wordt geblokkeerd en er wordt geen verder scannen uitgevoerd.
-5,9 t/m 0,0 (Neutraal)	monitor	De transactie wordt niet geblokkeerd op basis van Web Reputation, en zal worden uitgevoerd na contentcontroles (bestandstype en -grootte). Opmerking Sites zonder score worden bewaakt.

Wat betekent een ongecategoriseerde website?

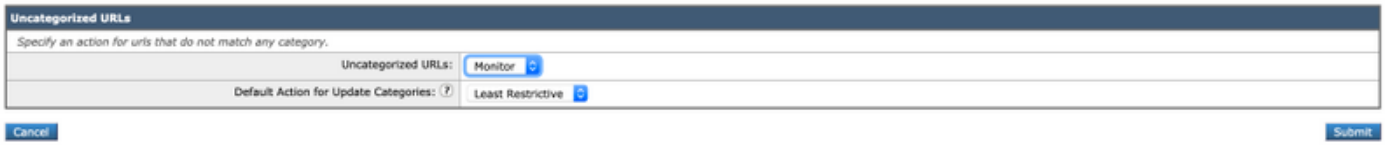
Niet gecategoriseerde URLS zijn degenen die de Databank van Cisco niet genoeg informatie over heeft om hun categorie te bevestigen. gewoonlijk pas opgerichte websites .

Hoe blokkeert u ongecategoriseerde URL's?

1. Ga naar het gewenste toegangsbeleid: **Web security Manager -> toegangsbeleid**.



2. Scrolt naar het gedeelte Ongecategoriseerde URL's.



3. Selecteer een van de gewenste handelingen, **monitor**, **Blok** of **waarschuwing**.

4. **Indienen** en **beloven van** wijzigingen.

Hoe vaak wordt de database bijgewerkt?

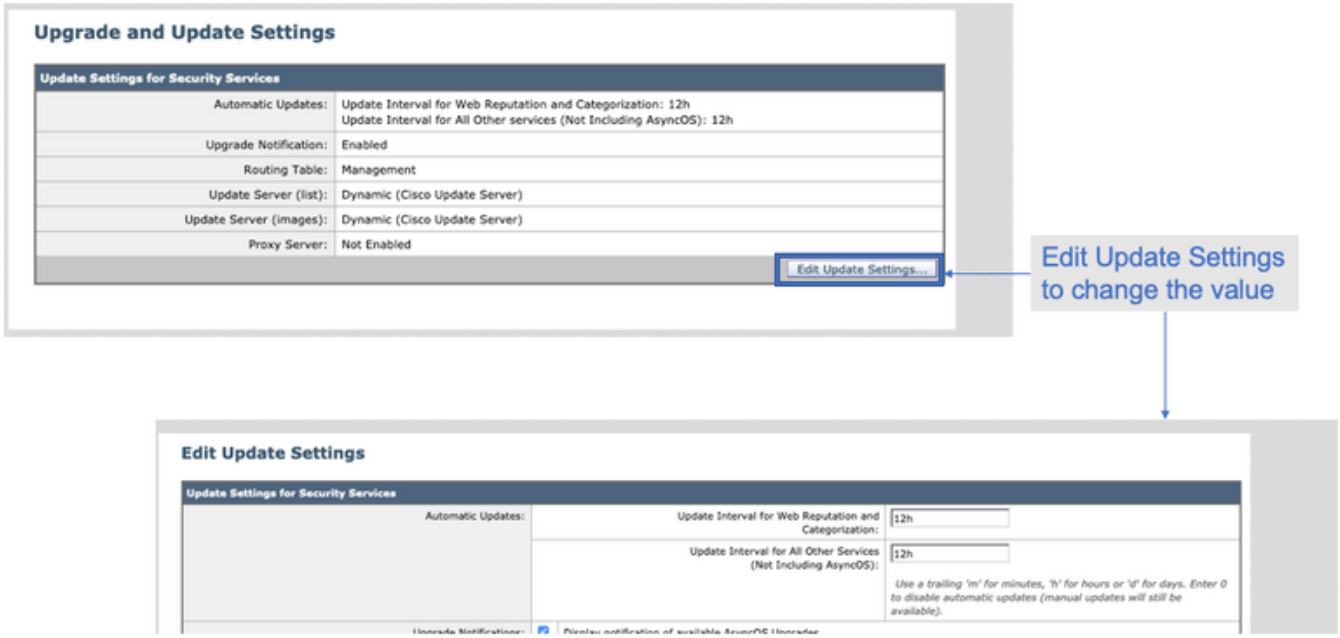
De frequentie van de updates kan worden bijgewerkt met behulp van de volgende opdracht van CLI: **updates**

```
WSA.local (SERVICE)> updateconfig

Service (images): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Update interval for Web Reputation and Categorization: 12h
Update interval for all other services: 12h

Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
The following services will use this routing table:
- Webroot
- Web Reputation Filters
- L4 Traffic Monitor
- Cisco Web Usage Controls
- McAfee
- Sophos Anti-Virus definitions
- Timezone rules
- HTTPS Proxy Certificate Lists
- Cisco AsyncOS upgrades

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
```

```
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

Opmerking: de bovenstaande waarde laat zien hoe vaak we op updates controleren , maar niet hoe vaak we nieuwe actualiseringen voor de reputatie en andere diensten publiceren . de bijgewerkte gegevens kunnen op elk moment beschikbaar zijn .

OF UIT GUI: **Systeembeheer -> Instellingen voor upgrade en updates.**



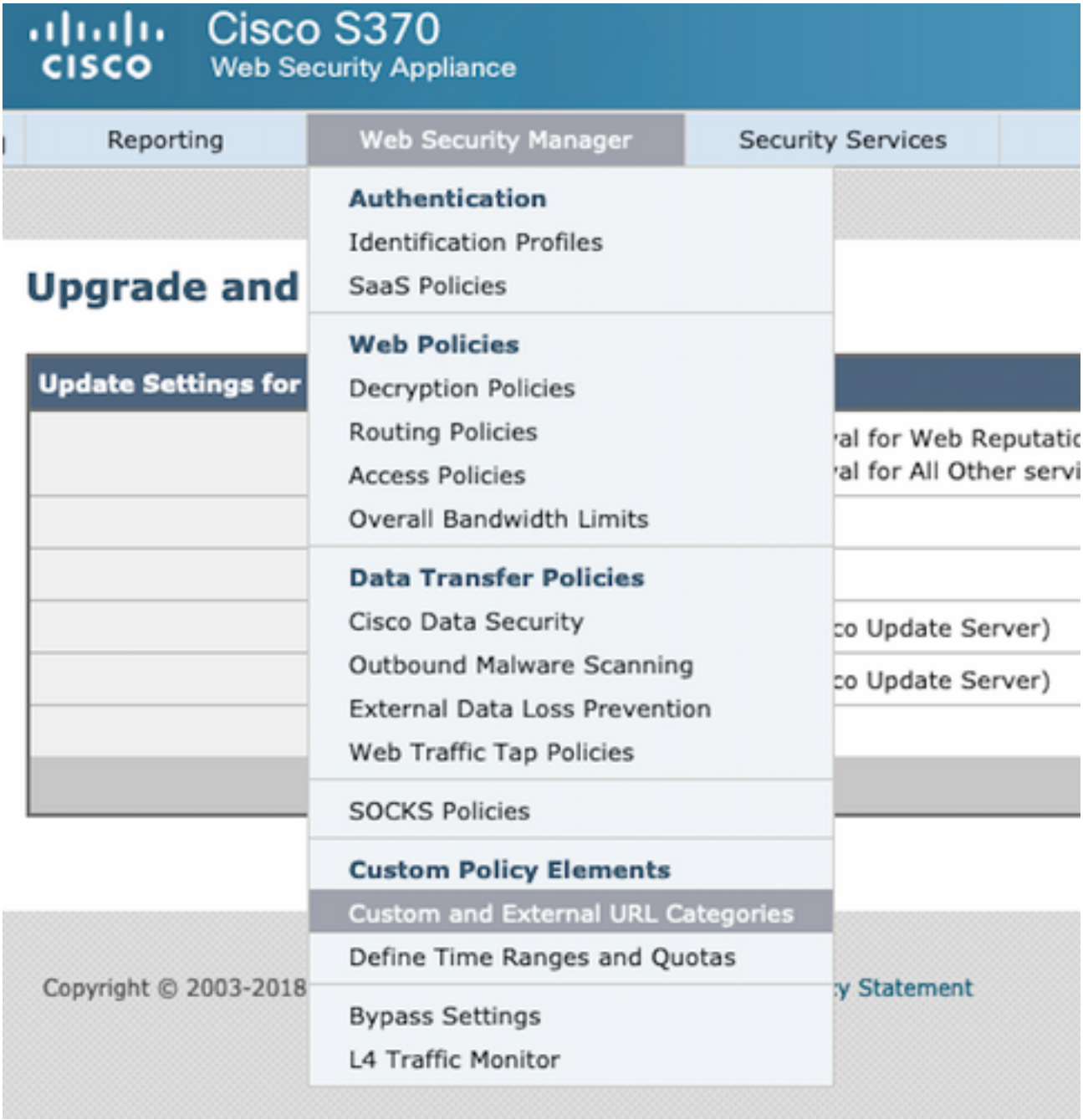
Hoe kan een URL door een witte of zwarte lijst worden geplaatst?

Soms kost het updates voor URLs van Cisco TALOS tijd, of door gebrek aan genoeg informatie. of er is geen manier om de reputatie te veranderen omdat de website nog steeds niet aantoonde dat het slecht gedrag veranderde . Op dit punt kunt u deze URL aan een aangepaste URL categorie toevoegen die uw toegangsbeleid toestaat/blokkeert of uw decryptie beleid doorlaat/laat vallen, en die de URL zonder het scannen of URL filteren controle door het Cisco Web Security Appliance (WSA) of blok garandeert.

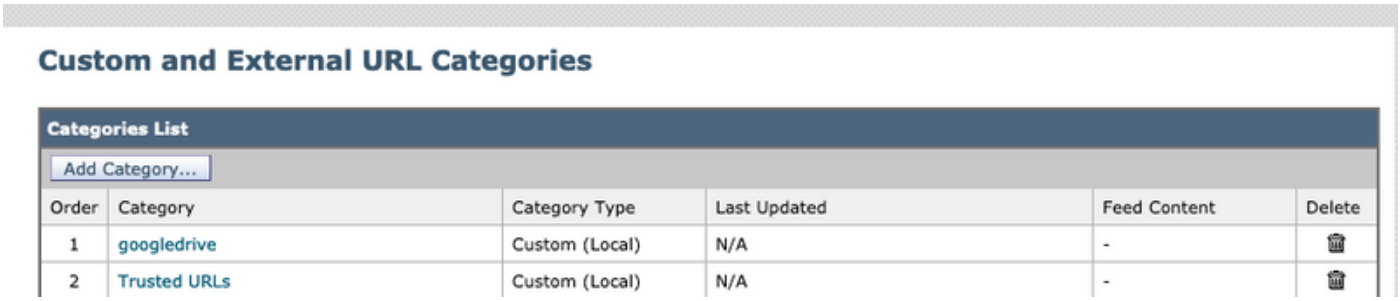
Volg voor Whitelist/Blacklist de volgende stappen:

1. Voeg URL toe in aangepaste URL categorie.

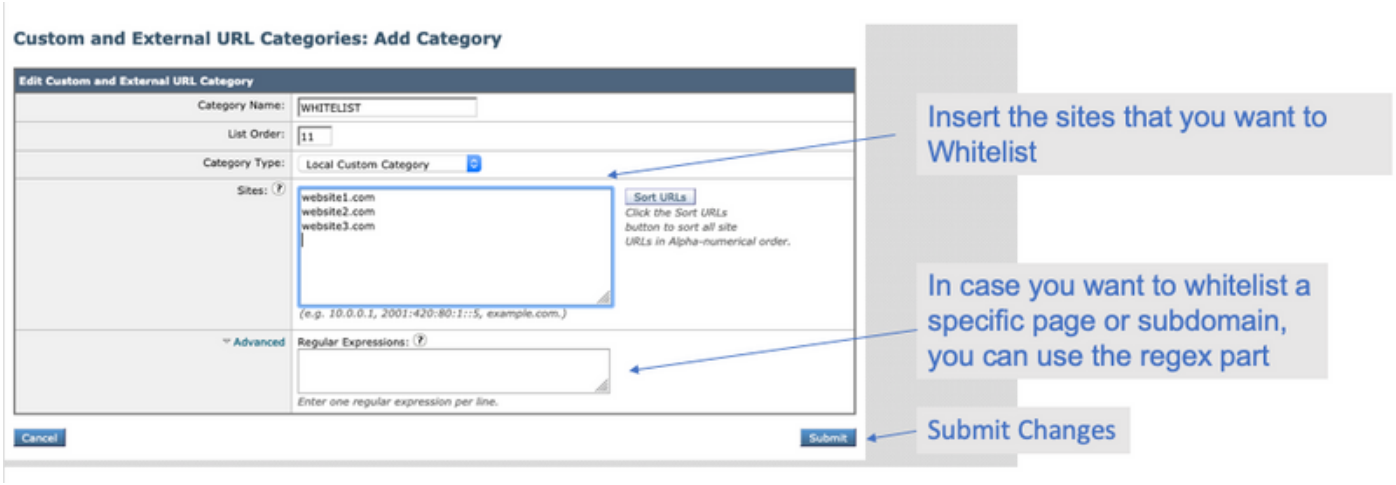
Ga van de GUI naar **Web Security Manager** -> **Aangepaste en externe URL-categorie**.



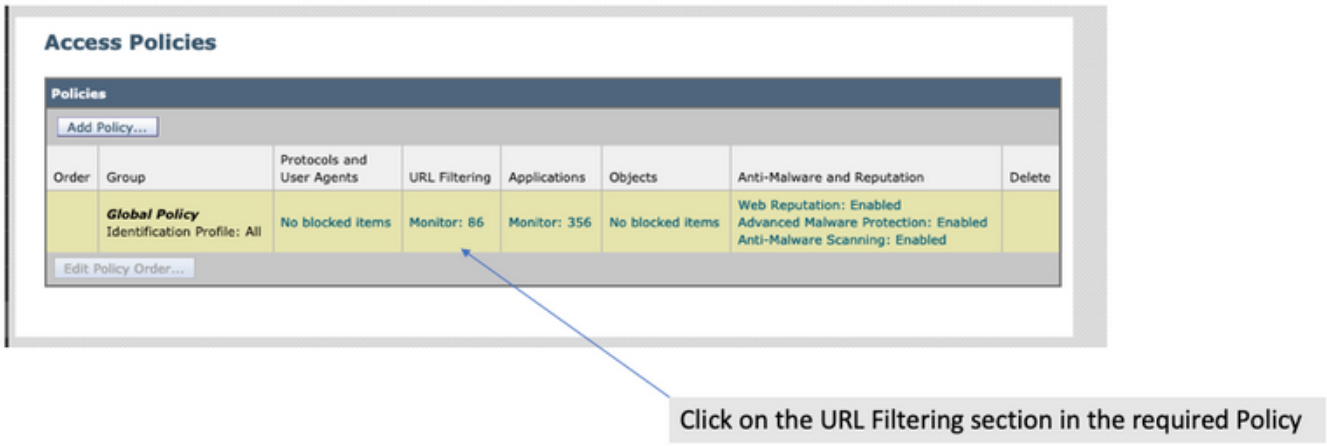
2. Klik op **categorie toevoegen**:



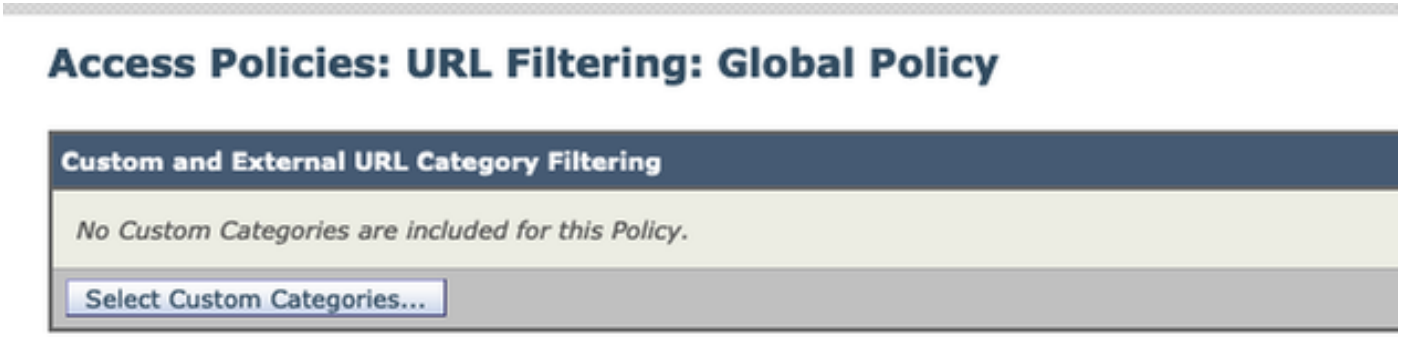
3. Voeg de websites toe die vergelijkbaar zijn met de screenshots hieronder:



4. Ga naar de URL-filtering in het gewenste toegangsbeleid (**Web security Manager -> toegangsbeleid -> URL-filtering**).

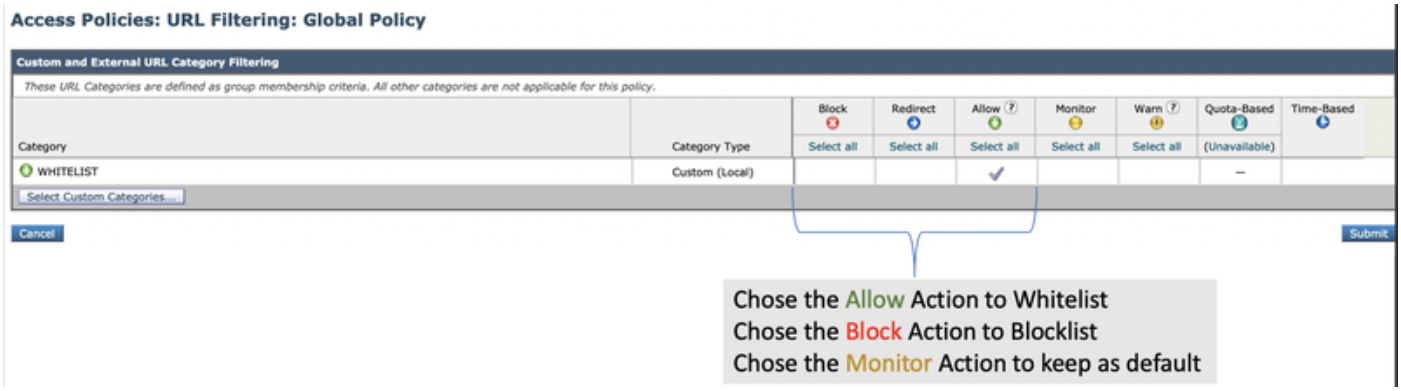


5. Selecteer de **WHITELIST of BLACKLIST** die we net hebben gecreëerd en neem deze op in het beleid.



6. Voeg de beleidscategorie toe in de URL-filterinstellingen van het beleid zoals hieronder.

7. Defineer de actie, Blok naar Blocklist, sta toe aan Whitelist. en als u wilt dat de URL door de scanmotoren gaat, behoudt u de Actie als monitor.



8. **Vermeld** en **verbind** wijzigingen.