Web Reputation Score (WBRS) und Web Kategorization Engine Häufig gestellte Fragen (FAQs)

Inhalt

Web Reputation Score (WBRS) und Web Kategorization Engine Frequently Asked Questions (FAQ).

In diesem Artikel werden die am häufigsten gestellten Fragen zur Webreputations-Bewertung (WBRS) und zur Kategorisierung mit der Cisco Web Security Appliance (WSA) beschrieben.

Was bedeutet Webreputations-Bewertung?

Webreputations-Filter weisen einer URL eine webbasierte Reputationsbewertung (WBRS) zu, um die Wahrscheinlichkeit zu ermitteln, dass URL-basierte Malware enthalten ist. Die Web Security Appliance verwendet Web-Reputationsbewertungen, um Malware-Angriffe zu erkennen und zu

stoppen, bevor sie auftreten. Sie können Webreputations-Filter mit Zugriffs-, Entschlüsselungs- und Cisco Datensicherheitsrichtlinien verwenden.

Was bedeutet Web-Kategorisierung?

Die Internet-Websites sind Kategorien, die auf dem Verhalten und dem Zweck dieser Websites basieren. Um es den Administratoren der Proxys zu erleichtern, haben wir jede Website-URL zu einer vordefinierten Kategorie hinzugefügt, in der sie zu Sicherheits- und Berichtszwecken identifiziert werden können. die Websites, die nicht zu einer der vordefinierten Kategorien gehören, werden als nicht kategorisierte Websites bezeichnet, die aufgrund der Erstellung neuer Websites und des Mangels an genügend Daten/Datenverkehr, um ihre Kategorie zu bestimmen. und das ändert sich mit der Zeit.

Wie finde ich Reputationsbewertung in Zugriffsprotokollen?

Jede Anfrage, die Sie über die Cisco Web Security Appliance (WSA) stellen, sollte eine Web-Based Reputation Score (WBRS)-Bewertung und eine URL-Kategorie aufweisen. und eine Möglichkeit, diese anzuzeigen, ist über die Zugriffsprotokolle. Das Beispiel unten: die WBRS-Bewertung (Web-Based Reputation Score) lautet (-1,4), und die URL-Kategorie lautet: Computer und Internet.

Textreferenz für den obigen Screenshot.

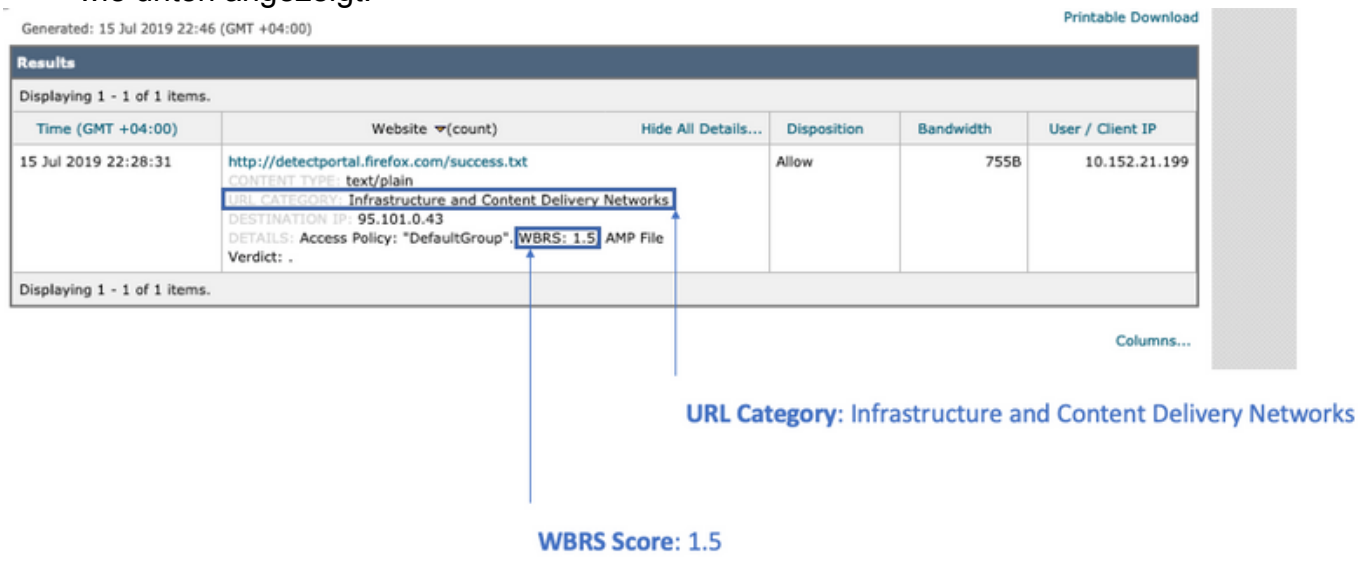
1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE ,0,"-",0,0,0,-,"-",-,-,-,"-","-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-",-,"-",-,-,"-",-,-,"-",->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

Hinweise:

- Zugriffsprotokolle können entweder über die Befehlszeilenschnittstelle (CLI) angezeigt oder heruntergeladen werden, indem eine Verbindung über die FTP-Methode (File Transfer Protocol) der IP-Verwaltungsschnittstelle hergestellt wird. (Stellen Sie sicher, dass FTP auf der Schnittstelle aktiviert ist.)
- Vollständige Liste der Kategorien Abkürzung: 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

Wie finde ich Reputationsbewertung in meinen Berichten?

1. Navigieren Sie zur **GUI** der Cisco Web Security Appliance (WSA) -> **Reporting** -> **Web Tracking**.
2. Suchen Sie nach der **Domäne**, die Sie suchen.
3. Klicken Sie auf der Seite **Ergebnisse** auf den gewünschten Link, und weitere Details werden wie unten angezeigt.



Wo prüfen Sie die WBRS-Aktualisierungsprotokolle (Web-Based Reputation Score)?

Web-Based Reputation Score (WBRS)-Aktualisierungsprotokolle finden Sie unter updater_logs. Sie können diese Protokolle über die FTP-Anmeldung (File Transfer Protocol) auf die Verwaltungsschnittstelle herunterladen. oder über die Befehlszeilenschnittstelle (CLI).

So zeigen Sie Protokolle mit Terminal an:

1. Öffnen Sie **Terminal**.
2. Geben Sie den Befehl **tail ein**.
3. Wählen Sie die **Protokollnummer aus** (diese hängt von der Version und der Anzahl der konfigurierten Protokolle ab).
4. Die Protokolle werden angezeigt.

```
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
```

Wie überprüfen Sie, ob eine Verbindung zu besteht? Webbasierte Reputationsbewertung (WBRS) Server aktualisieren?

Um sicherzustellen, dass Ihre Cisco Web Security Appliance (WSA) die neuen Aktualisierungen erhalten kann. Stellen Sie sicher, dass die Verbindung zu den Servern von Cisco Update über die folgenden TCP-Ports 80 und 443 verfügbar ist:

```
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 '^]'.
```

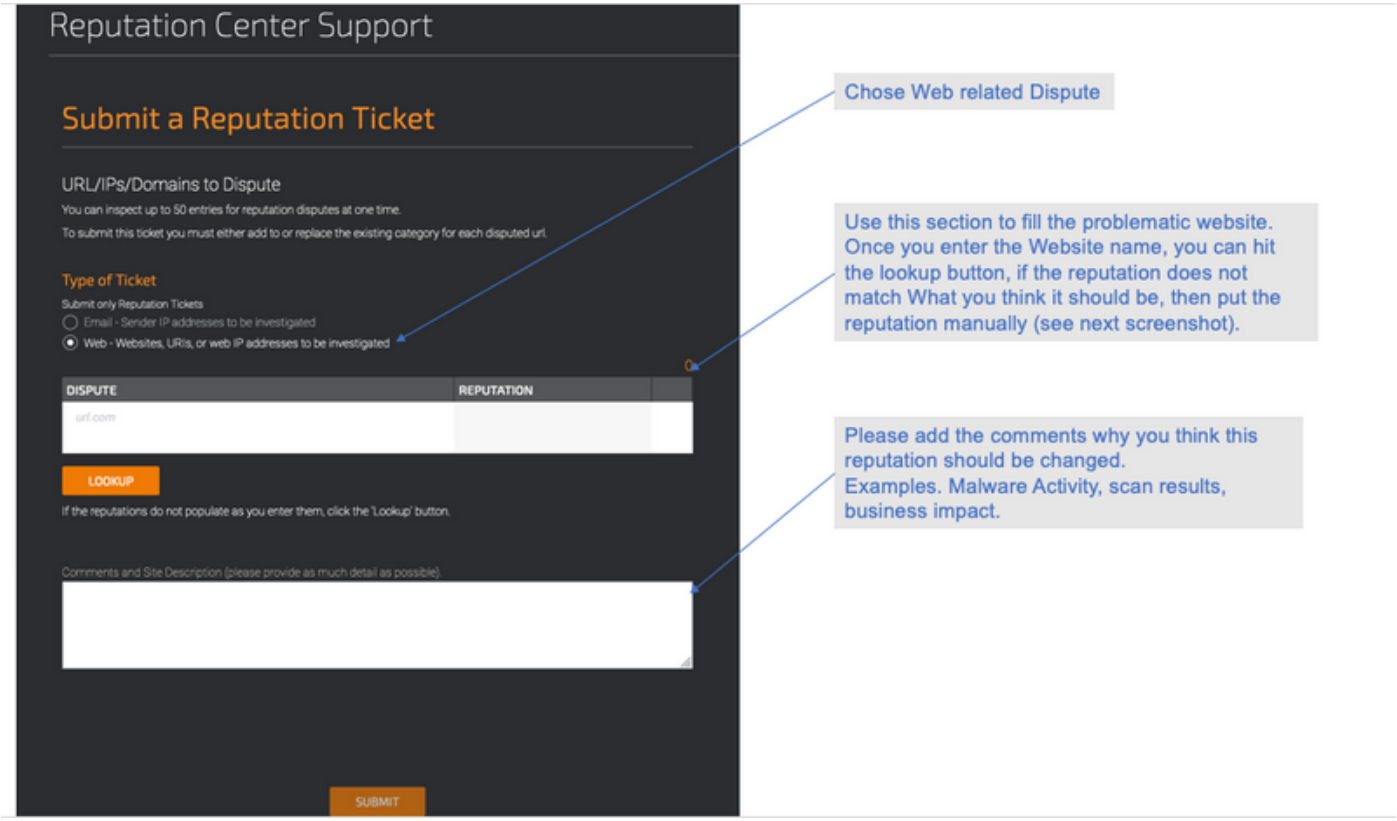
> **Hinweis**: Wenn Sie einen Upstreamproxy haben, führen Sie die obigen Tests über Ihren Upstream-Proxy durch.

Wie können Sie einen Streit zur Web-Kategorisierung einreichen?

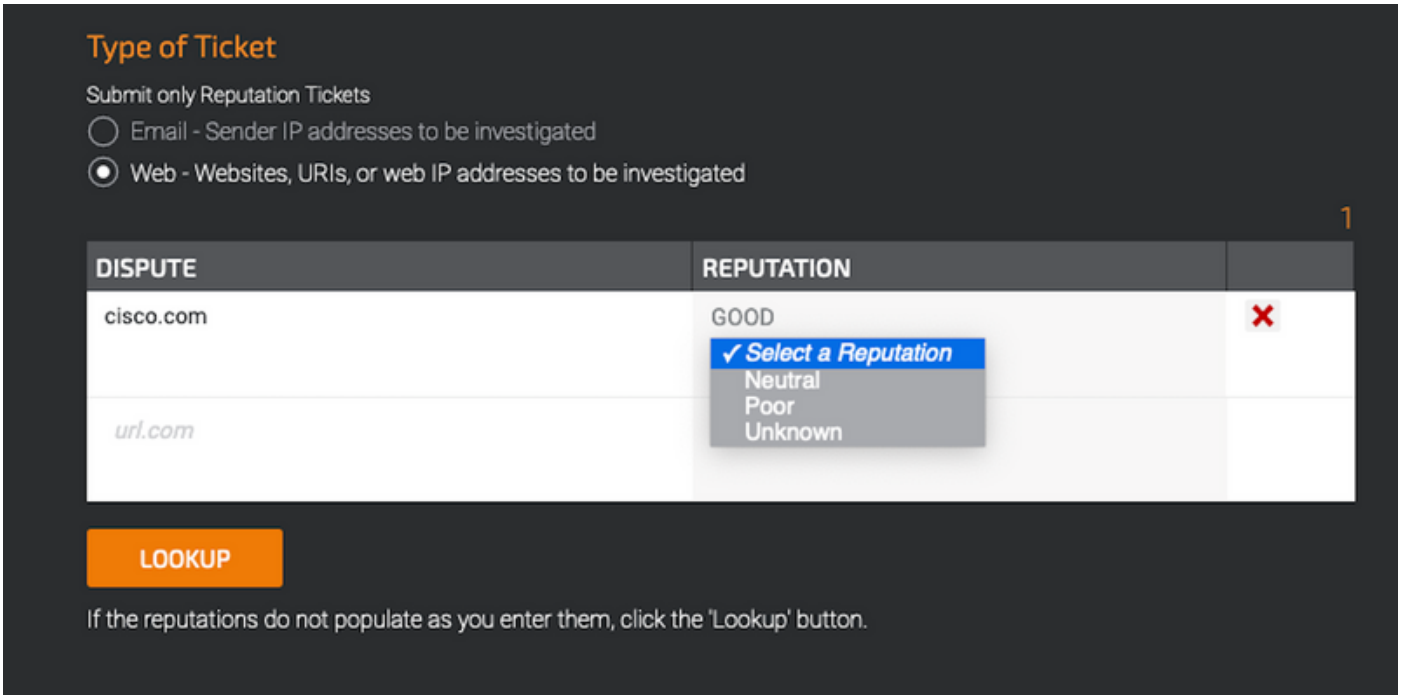
Nachdem überprüft wurde, dass sowohl die Cisco Web Security Appliance (WSA) als auch Cisco TALOS die gleiche Reputationsbewertung aufweisen, Sie jedoch immer noch der Meinung sind, dass dies kein gültiges Ergebnis ist, müssen Sie dies durch Einreichen einer Streitigkeit mit dem Cisco TALOS-Team beheben.

Dies kann über den folgenden Link erfolgen:
https://talosintelligence.com/reputation_center/support

Um den **Streitfall einzusenden**, befolgen Sie bitte die nachstehenden Anweisungen.



Die Ergebnisse nach dem Klicken auf "Suchen" und die Option, die Punktzahl manuell zu ändern.



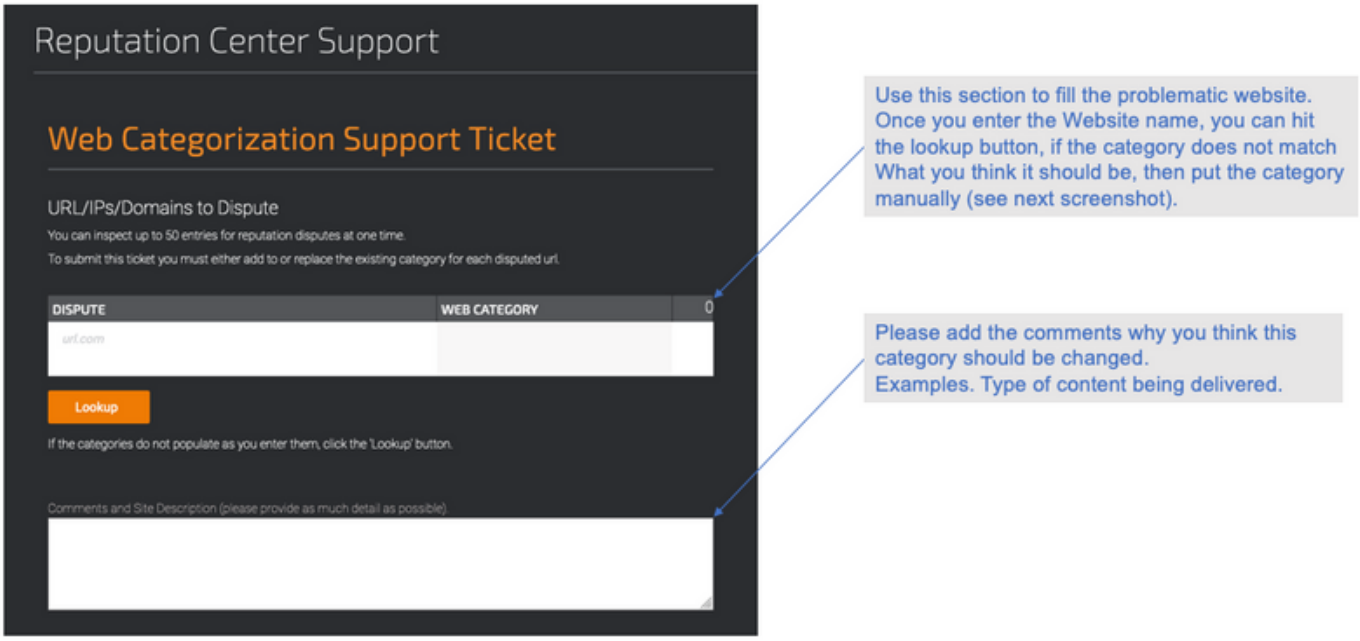
Hinweis: Einsendungen von Cisco TALOS können einige Zeit in der Datenbank enthalten sein. Wenn das Problem dringlich ist, können Sie immer eine **WHITELIST** oder **BLOCKLIST** erstellen, bevor das Problem im Cisco Backend behoben wird. Dazu können Sie diesen Abschnitt (How To Whitelist oder BlackList URL) überprüfen.

Wie werden Streitigkeiten für die Webreputations-Bewertung eingereicht?

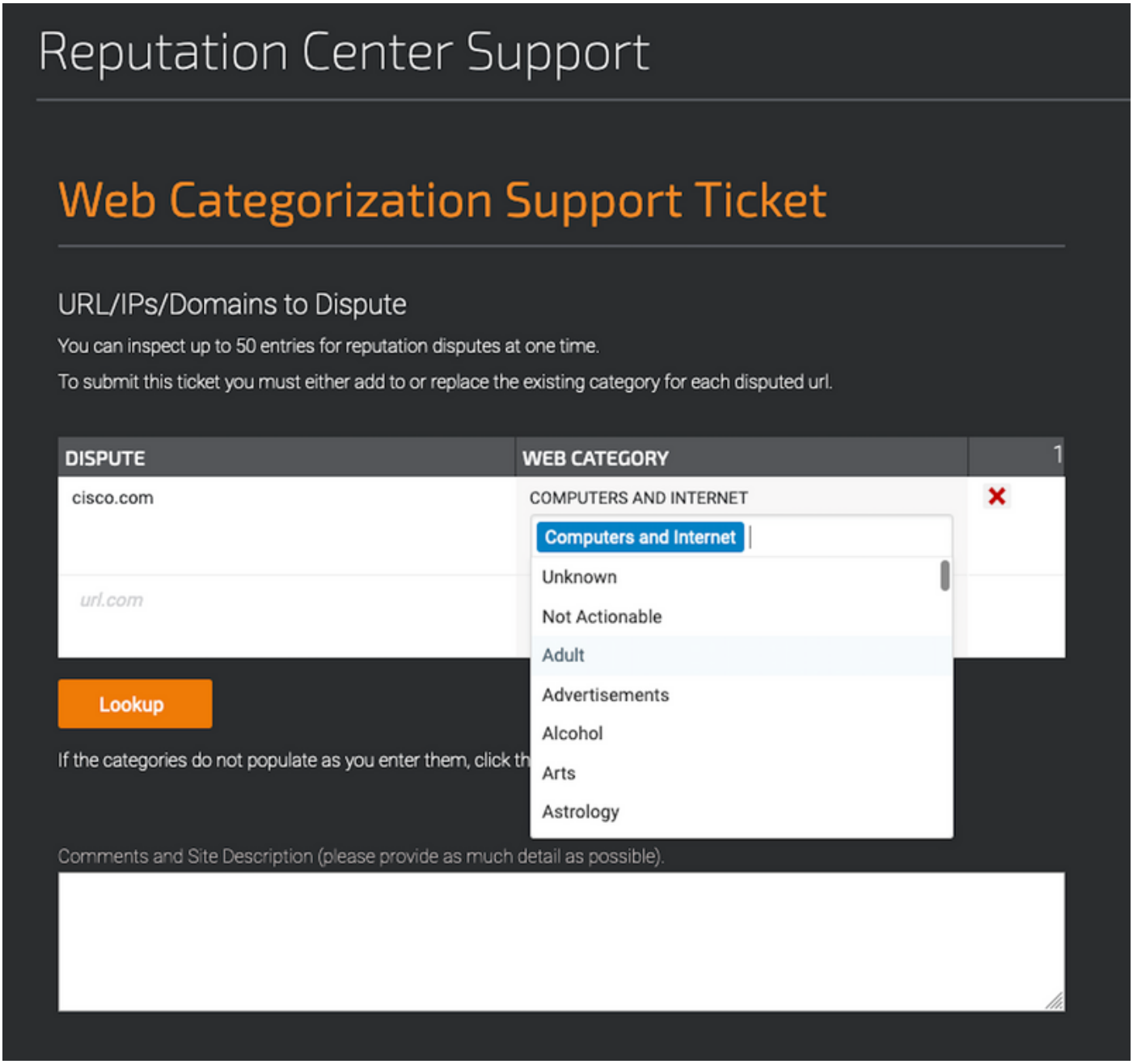
Nachdem überprüft wurde, dass sowohl die Cisco Web Security Appliance (WSA) als auch Cisco TALOS die gleiche Kategorisierung aufweisen, Sie jedoch immer noch der Meinung sind, dass dies kein gültiges Ergebnis ist, müssen Sie dies mit dem Cisco TALOS-Team besprechen.

Rufen Sie die Seite zum Einsenden von Kategorisierungen auf der TALOS-Website auf: https://talosintelligence.com/reputation_center/support#categorization

Um den **Streitfall einzusenden**, befolgen Sie bitte die nachstehenden Anweisungen.



Um die Kategorie zu aktualisieren, wählen Sie aus dem **Dropdown-**Menü aus, was die Website Ihrer Meinung nach besser anpasst, und achten Sie darauf, dass Sie die Kommentarrichtlinien befolgen.



Es wurde eine Anfechtung eingereicht, die Bewertung oder Kategorie wird jedoch nicht auf der Cisco Web Security Appliance (WSA) oder Cisco TALOS aktualisiert.

Falls Sie ein Ticket bei Cisco TALOS eingereicht haben und die Reputation/Bewertung nicht innerhalb von 3-4 Tagen aktualisiert wurde. Sie können Ihre Update-Einstellungen überprüfen und sicherstellen, dass Sie auf den Cisco Update-Server zugreifen können. Wenn alle diese Schritte in Ordnung sind, können Sie ein Ticket beim Cisco TAC erstellen. Der Cisco Techniker wird Ihnen bei der Kontaktaufnahme mit dem Cisco TALOS-Team behilflich sein.

> **Hinweis**: Sie können die WHITELIST/BLOCKLIST-Arbeitsumgehung anwenden, um die gewünschte Aktion anzuwenden, bis die Kategorie/Reputation vom Cisco TALOS-Team aktualisiert wird.

Cisco Web Security Appliance (WSA) zeigt andere Ergebnisse als Cisco TALOS an. Wie kann das behoben werden?

Die Datenbank kann auf der Cisco Web Security Appliance (WSA) aus mehreren Gründen veraltet sein. Dies gilt hauptsächlich für die Kommunikation mit unseren Aktualisierungsservern. Bitte befolgen Sie diese Schritte, um sicherzustellen, dass Sie die richtigen Aktualisierungsserver und die richtige Verbindung haben.

1. Überprüfen Sie, ob die Verbindung für die Server der Cisco Updates an den Ports 80 und 443 vorhanden ist:

```
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. Wenn Sie einen Upstreamproxy haben, stellen Sie sicher, dass der Upstream-Proxy die oben genannten Tests über den Upstream-Proxy durchführt.

3. Wenn die Verbindung gut ist und Sie immer noch den Unterschied sehen, zwingen Sie die Updates manuell: **Aktualisiert** von der CLI oder von **GUI->Sicherheitsdiensten -> Malware-Schutz -> Aktualisiert**.

Warten Sie einige Minuten, und wenn das nicht funktioniert, überprüfen Sie den nächsten Schritt.

4. An dieser Stelle müssen Sie updater_logs überprüfen: offenes **Terminal: CLI->tail-> (Wählen Sie die Anzahl der Protokolldateien von updater_logs aus.)** Dadurch werden in den Aktualisierungsprotokollen nur die neuen Zeilen angezeigt.

Protokollzeilen sollten mit der Zeile "**Received Remote Command to signal a Manual update**" beginnen:

```
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. Suchen Sie nach "**Critical/Warning**"-Meldungen. Die Aktualisierungsprotokolle sind sehr von

Menschen lesbare Fehler und werden Sie höchstwahrscheinlich an der Stelle führen, an der das Problem liegt.

6. Wenn Sie keine Antwort erhalten haben, können Sie ein Ticket mit dem Cisco Support öffnen, das die Ergebnisse der oben genannten Schritte enthält. Der Kunde wird Ihnen gerne weiterhelfen.

Wie werden Web-Reputationsbewertungen berechnet?

Einige der Parameter, die bei der Zuweisung einer Punktzahl zu einer bestimmten Website berücksichtigt werden:

- URL-Kategorisierungsdaten
- Vorhandensein von herunterladbarem Code
- Vorhandensein langer, verschleierter Endbenutzer-Lizenzvereinbarungen (EULAs)
- Globales Volumen und Volumenänderungen
- Informationen zum Netzwerkbesitzer
- Verlauf einer URL
- Alter einer URL
- Präsenz auf allen Blocklisten
- Präsenz auf allen Zulassungslisten
- URL-Tippfehler beliebter Domänen
- Informationen zum Domänenregistrar
- IP-Adressinformationen

Wie hoch ist der Wertebereich für die einzelnen Reputationskategorien (gut, neutral, schlecht)?

Webreputations-Bereiche und zugehörige Aktionen:

Zugriffsrichtlinien:

Bewertung	Aktion	Beschreibung	Beispiel
-10 bis -6,0 (Schlecht)	Blockieren	Schlechte Seite. Die Anfrage wird blockiert, und keine weiteren Malware-Scans tritt ein.	• URL lädt Informationen ohne. • Benutzerberechtigungen. • plötzlicher Anstieg des URL-Volumens. • URL ist ein Typo einer beliebten Domäne..
-5,9 bis 5,9 (Neutral)	Scannen	Unbestimmte Website. Anfrage ist an die DVS-Engine für weitere Malware-Scans. Die DVS-Modul scannt die Anforderung und Serverantwortinhalte.	• Kürzlich erstellte URL, die eine • dynamische IP-Adresse und enthält • Inhalte herunterladen. • IP-Adresse des Netzwerkbesitzers mit • Positive Webreputations-Bewertung.
6,0 bis 10,0 (Gut)	Zulassen	Gute Website. Anfrage ist zulässig. Keine Malware-Prüfung erforderlich.	• URL enthält keine herunterladbaren Inhalte. • Replizierbare, großvolumige Domäne mit lan

			Geschichte. • Domäne in mehreren Zulassungslisten vorhar • Keine Links zu URLs mit schlechter Reputati

Entschlüsselungsrichtlinien:

Bewertung	Aktion	Beschreibung
-10 bis -9,0 (Schlecht)	Löschen	Schlechte Seite. Die Anfrage wird ohne Benachrichtigung an den Endbenutzer verworfen. Verwenden Diese Einstellung sollte mit Vorsicht verwendet werden.
-8,9 bis 5,9 (Neutral)	Entschlüsseln	Unbestimmte Website. Anfrage ist zulässig, Verbindung wird jedoch entschlüsselt und Zugriffsrichtlinien werden auf den entschlüsselten Datenverkehr angewendet.
6,0 bis 10,0 (Gut)	Durchleiten	Gute Website. Die Anforderung wird ohne Überprüfung oder Entschlüsselung weitergeleitet.

Cisco Datensicherheitsrichtlinien:

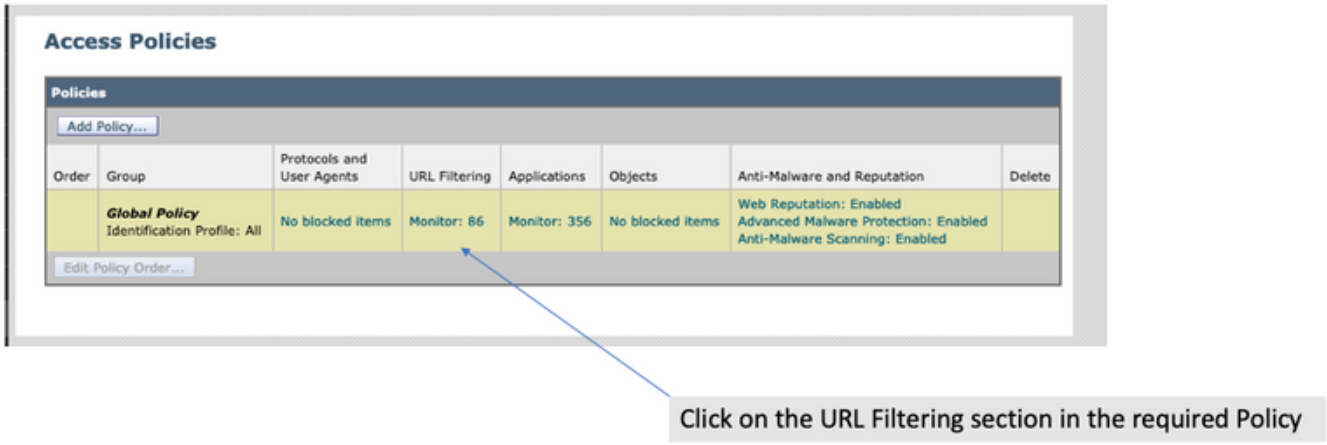
Bewertung	Aktion	Beschreibung
-10 bis -6,0 (Schlecht)	Blockieren	Schlechte Seite. Die Transaktion wird blockiert, und es wird kein weiterer Scanvorgang durchgefü
-5,9 bis 0,0 (Neutral)	Überwachung	Die Transaktion wird nicht aufgrund der Webreputation blockiert, und sie führt die Inhaltsprüfun (Dateityp und -größe) durch. Hinweis Standorte ohne Bewertung werden überwacht.

Was bedeutet nicht kategorisierte Website?

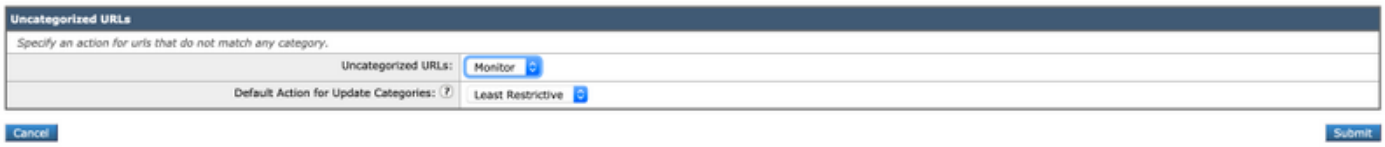
Nicht kategorisierte URLs sind solche, über die die Cisco Datenbank nicht genügend Informationen zur Bestätigung ihrer Kategorie verfügt. in der Regel neu erstellte Websites.

Wie blockieren Sie nicht kategorisierte URLS?

1. Gehen Sie zur gewünschten Zugriffsrichtlinie: **Web Security Manager -> Zugriffsrichtlinien**.



2. Blättern Sie nach unten zum Abschnitt Nicht kategorisierte URLs.



3. Wählen Sie eine der gewünschten Aktionen aus: **Überwachen**, **Blockieren** oder **Warnen**.

4. Änderungen **einsenden** und **bestätigen**

Wie häufig wird die Datenbank aktualisiert?

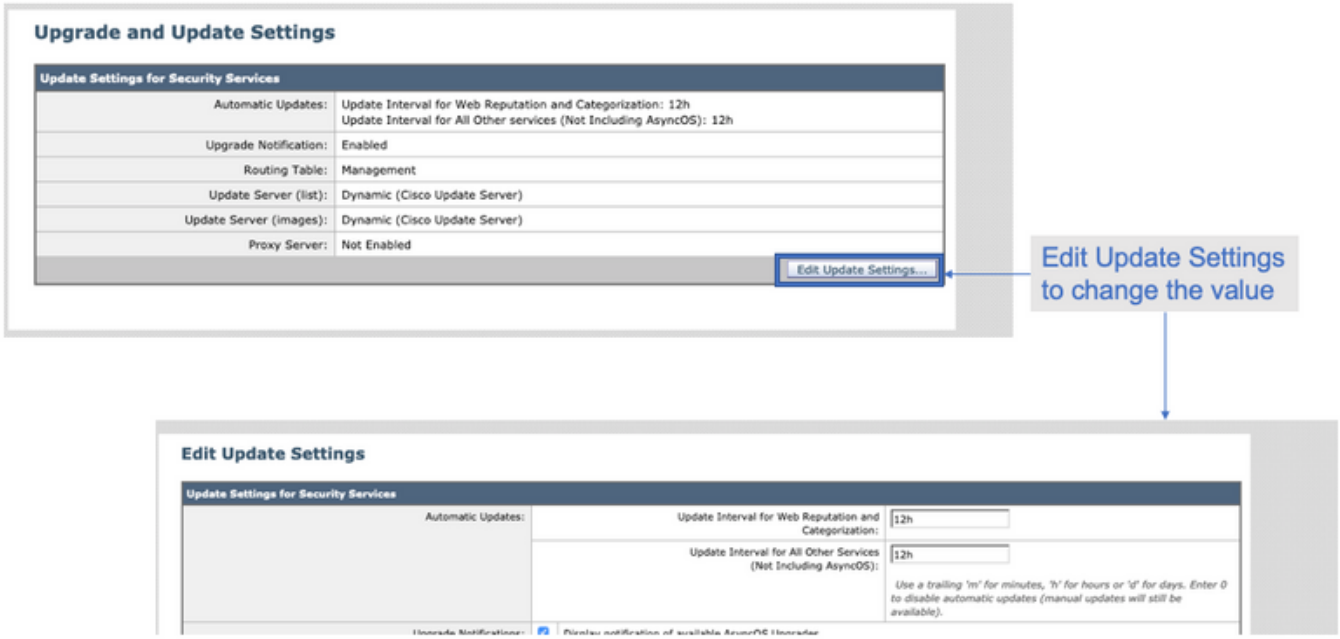
Die Aktualisierungshäufigkeit kann entweder mit dem folgenden CLI-Befehl aktualisiert werden: **updateconfig**

```
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
[]>
```

Hinweis: der obige Wert zeigt, wie häufig wir nach Updates suchen, aber nicht, wie häufig wir neue Updates für die Reputation und andere Dienste veröffentlichen. die Updates können jederzeit verfügbar sein.

ODER über GUI: **Systemverwaltung -> Upgrade- und Aktualisierungseinstellungen.**



Wie wird eine URL in einer Whitelist/Blacklist angezeigt?

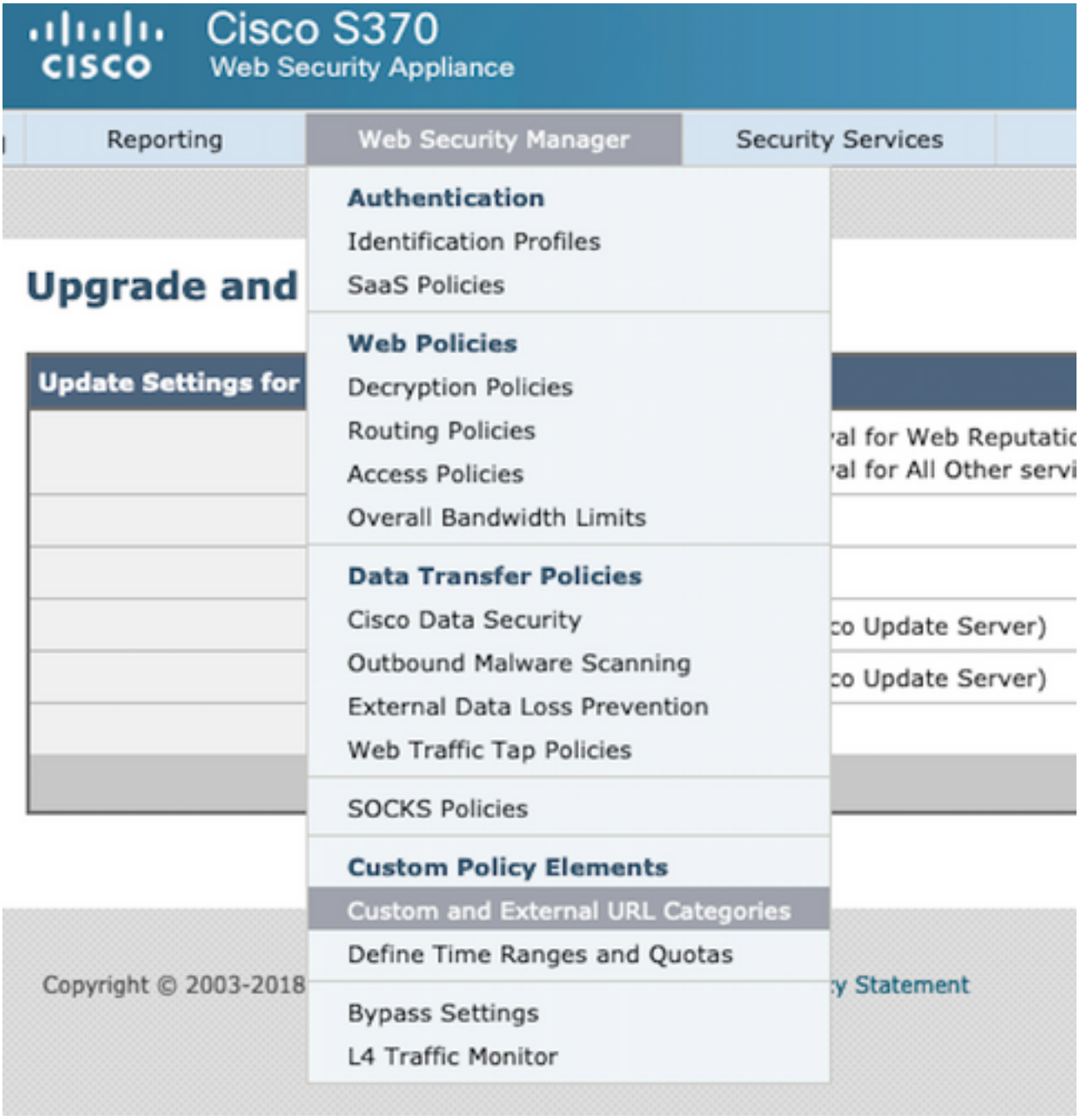
In manchen Fällen dauert die Aktualisierung von URLs von Cisco TALOS etwas länger, entweder aufgrund unzureichender Informationen. oder es gibt keine Möglichkeit, die Reputation zu ändern,

da die Website die Änderung des schädlichen Verhaltens noch nicht nachgewiesen hat. an dieser Stelle können Sie diese URL einer benutzerdefinierten URL-Kategorie hinzufügen, die in Ihren Zugriffsrichtlinien zugelassen/blockiert oder Ihre Entschlüsselungsrichtlinie weitergegeben/deaktiviert. Dadurch wird sichergestellt, dass die URL ohne Prüfung oder URL-Filterung durch die Cisco Web Security Appliance (WSA) oder den Block bereitgestellt wird.

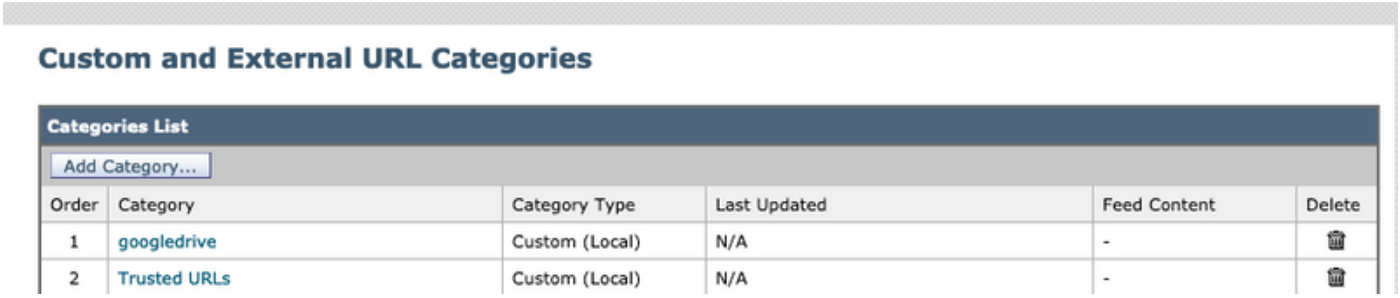
Um eine Whitelist/Blacklist-URL zu erhalten, gehen Sie wie folgt vor:

1. URL in benutzerdefinierte URL-Kategorie hinzufügen

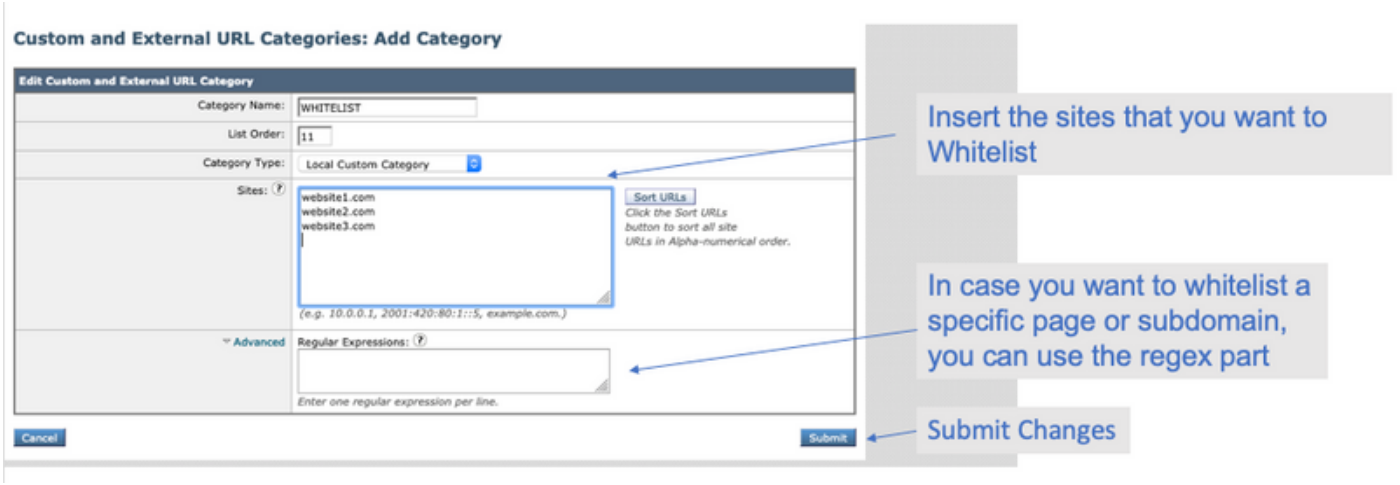
Gehen Sie von der GUI zum **Web Security Manager** -> **Benutzerdefinierte und externe URL-Kategorie**.



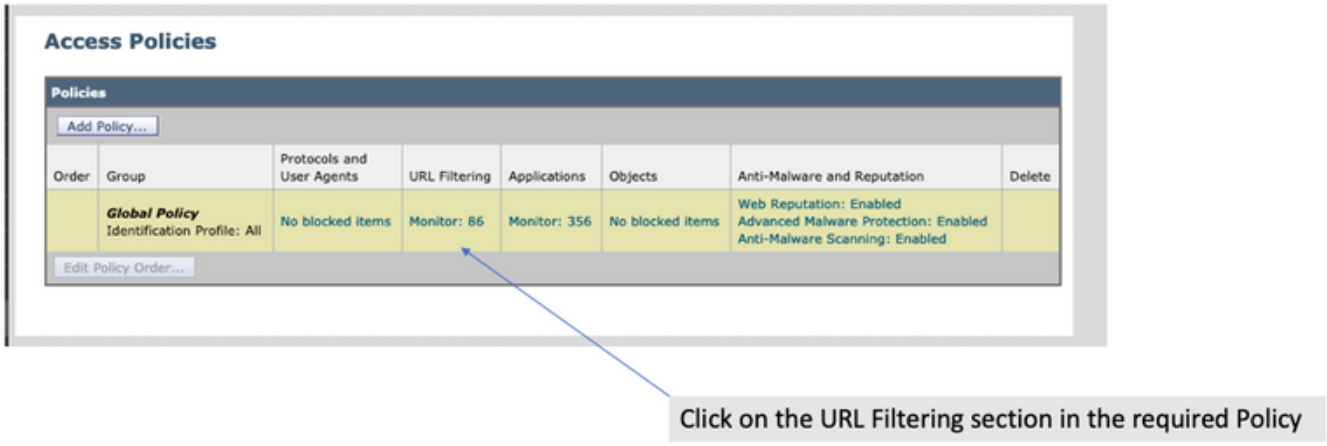
2. Klicken Sie auf **Kategorie hinzufügen**:



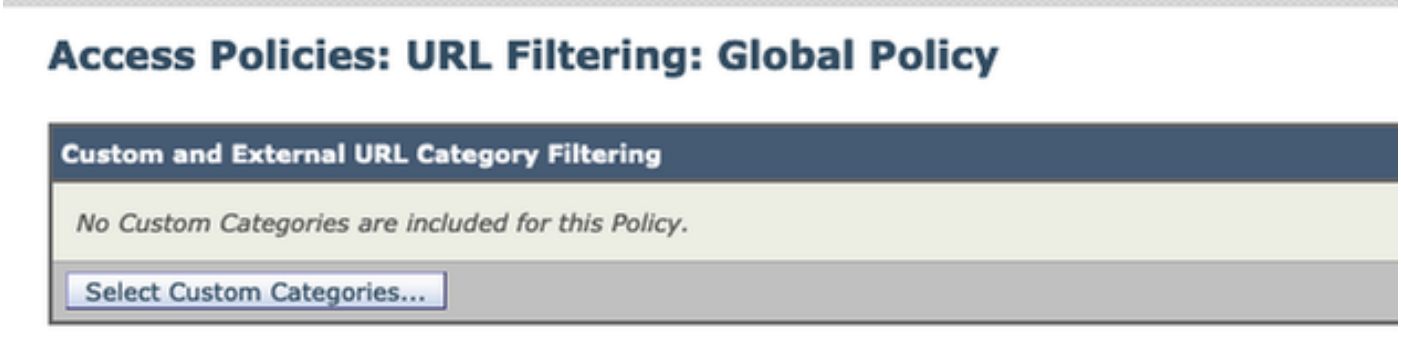
3. Fügen Sie die Websites ähnlich den Screenshots unten hinzu:



4. Gehen Sie in der erforderlichen Zugriffsrichtlinie zur URL-Filterung (**Websicherheits-Manager -> Zugriffsrichtlinien -> URL-Filterung**).

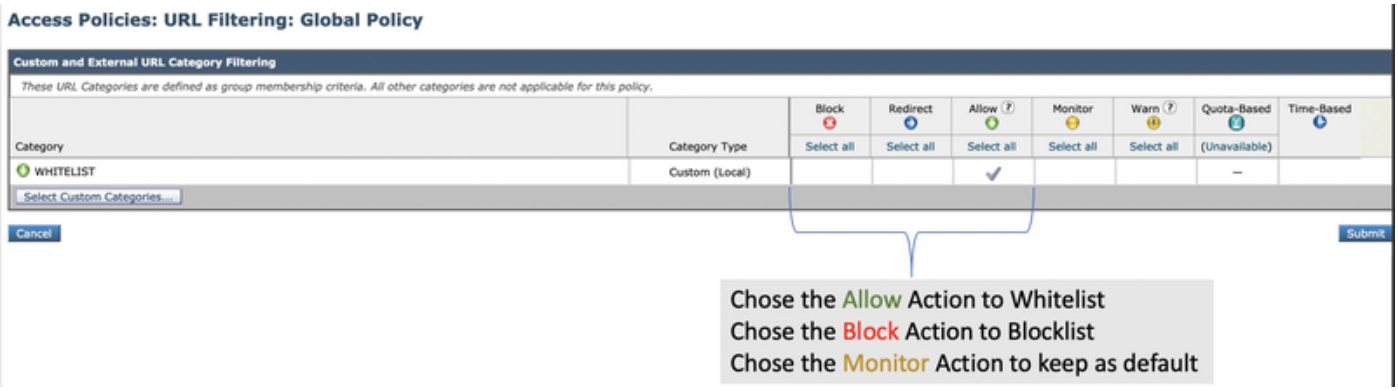


5. Wählen Sie die **WHITELIST oder BLACKLIST aus**, die wir gerade erstellt haben, und fügen Sie sie in die Richtlinie ein.



6. Integrieren Sie die Richtlinienkategorie wie unten in den Einstellungen für die URL-Filterung der Richtlinie.

7. Definieren Sie die Aktion, Block to Blocklist, Allow to Whitelist. und wenn Sie möchten, dass die URL durch die Scan-Engines geleitet wird, behalten Sie die Aktion als Überwachen bei.



8. Änderungen **einsenden** und **bestätigen**.