웹 평판 점수(WBRS) 및 웹 분류 엔진 FAQ(자주 묻는 질문)

목차

(WBRS) FAQ( )

이 문서에서는 Cisco WSA(Web Security Appliance)를 통한 WBRS(Web Reputation Score) 및 분류 기능에 대한 가장 자주 묻는 질문에 대해 설명합니다.

웹 평판 점수의 의미

웹 평판 필터는 URL에 WBRS(Web-Based Reputation Score)를 할당하여 URL 기반 악성코드를 포함할 가능성을 확인합니다.Web Security Appliance는 웹 평판 점수를 사용하여 악성코드 공격이 발생하기 전에 이를 식별하고 차단합니다.웹 평판 필터를 액세스, 암호 해독 및 Cisco 데이터 보안 정책과 함께 사용할 수 있습니다.

웹 분류란 무엇을 의미합니까?

인터넷 웹 사이트는 이러한 웹 사이트의 동작 및 목적을 기반으로 하는 범주이며, 프록시의 관리자

가 쉽게 사용할 수 있도록 모든 웹 사이트 URL을 사전 정의된 카테고리에 추가했으며, 이 카테고리는 보안 및 보고 목적으로 식별될 수 있습니다.미리 정의된 카테고리 중 하나에 속하지 않는 웹 사이트를 분류되지 않은 웹 사이트라고 합니다. 이는 새로운 웹 사이트를 만들고 데이터/트래픽이 부족하여 카테고리를 확인할 수 없기 때문일 수 있습니다.시간이 지남에 따라 변경됩니다.

액세스 로그에서 평판 점수를 찾는 방법

Cisco WSA(Web Security Appliance)를 통해 수행하는 모든 요청에는 WBRS(Web-Based Reputation Score) 점수와 URL 카테고리가 연결되어 있어야 합니다.액세스 로그를 통해 이를 확인하는 방법 중 하나는 다음과 같습니다.WBRS(Web-Based Reputation Score) 점수는 (-1.4)이고 URL 범주는 다음과 같습니다.컴퓨터와 인터넷.

위 스크린샷에 대한 텍스트 참조입니다.

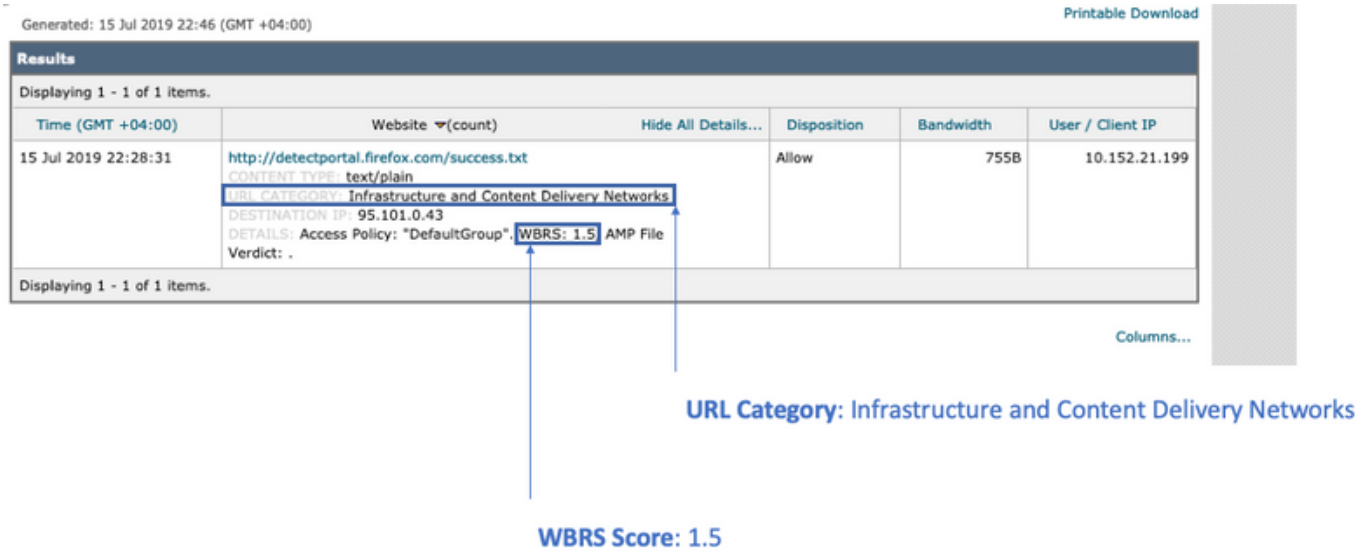
1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE ,0,"-",0,0,0,-,"-",-,-,-,"-","-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-",-,"-","-",-,-,"-","-",-,-,"-",->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

참고:

- 액세스 로그는 CLI(Command Line Interface)에서 보거나 관리 인터페이스 IP에서 FTP(File Transfer Protocol) 메서드를 사용하여 연결하여 다운로드할 수 있습니다(인터페이스에서 FTP가 활성화되었는지 확인).
- 범주 약어의 전체 목록: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

보고서에서 평판 점수를 찾는 방법

1. Cisco WSA(Web Security Appliance) **GUI** -> **Reporting** -> **Web Tracking** .
2. .
3. .



웹 기반 평판 점수(WBRS) 업데이트 로그는 어디에서 확인합니까?

WBRS(Web-Based Reputation Score) 업데이트 로그는 updater_logs 아래에서 찾을 수 있으며, 관리 인터페이스에 대한 FTP(File Transfer Protocol) 로그인을 통해 이러한 로그를 다운로드할 수 있습니다.또는 CLI(Command Line Interface)를 통해 확인할 수 있습니다.

터미널을 사용하여 로그를 보려면

1. 터미널을 **엽니다**.
2. 명령 **테일**을 **입력합니다**.
3. **로그 번호**를 선택합니다(버전 및 구성된 로그 수에 따라 다름).
4. 로그가 표시됩니다.

```
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
```

연결 대상 웹 기반 평판 점수(WBRS) 업데이트 서버

Cisco WSA(Web Security Appliance)에서 새 업데이트를 가져올 수 있는지 확인합니다.다음 TCP(Transmission Control Protocol) 포트 80 및 443에서 Cisco 업데이트의 서버에 연결되었는지 확인하십시오.

```
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 '^]'.
```

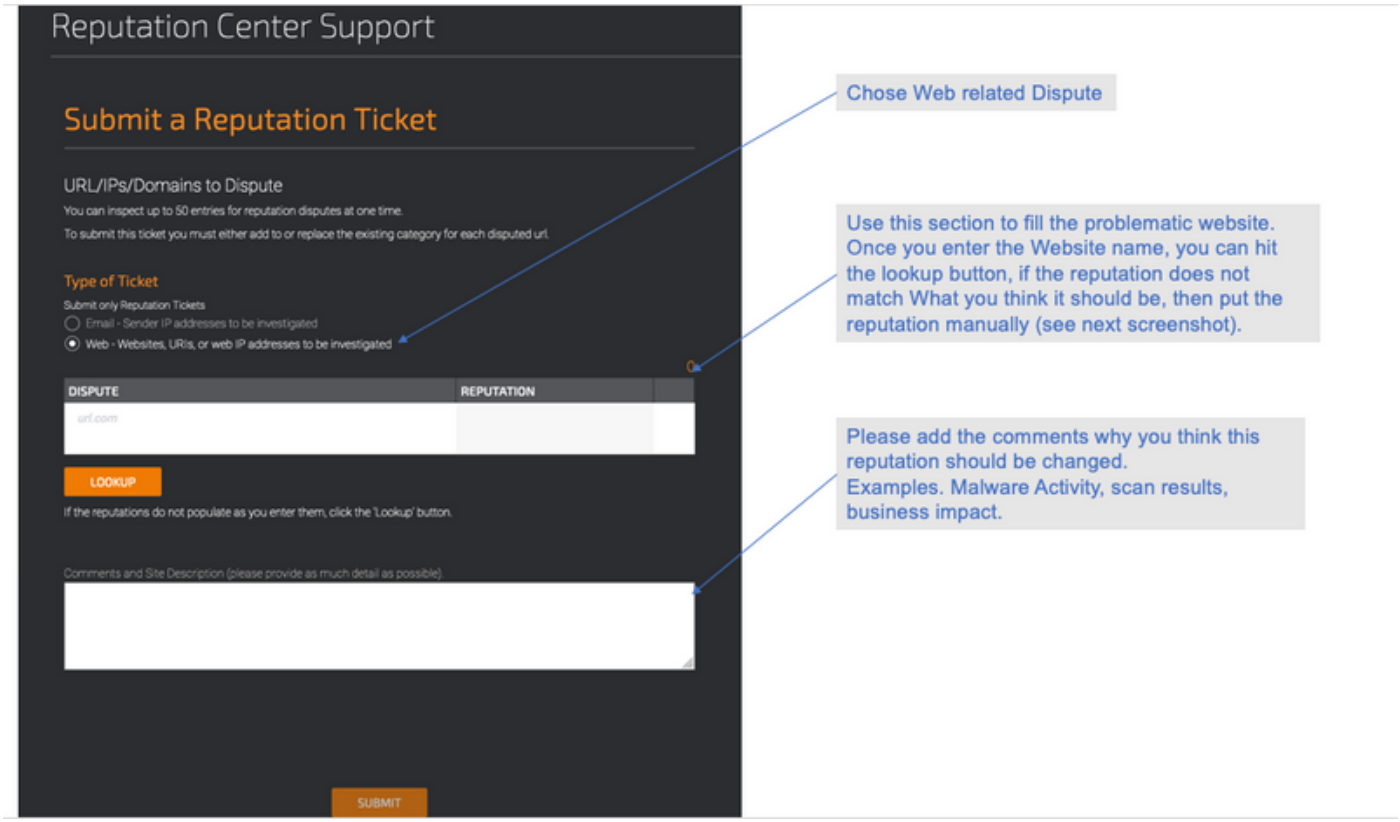
참고:업스트림 프록시가 있는 경우 업스트림 프록시를 통해 위의 테스트를 수행합니다.

웹 분류에 대한 분쟁은 어떻게 제기합니까?

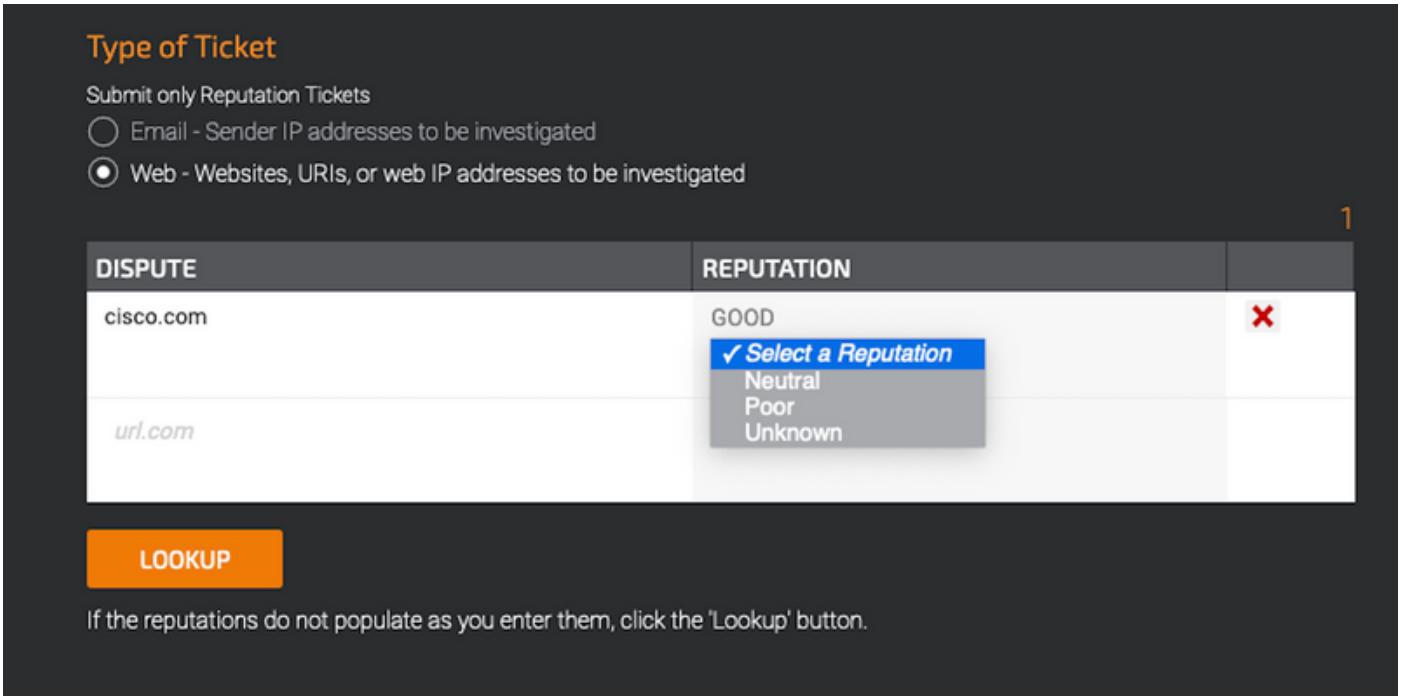
Cisco WSA(Web Security Appliance) 및 Cisco TALOS 모두 평판 점수가 동일한지 확인한 후, 이 결과가 유효한 결과가 아니라고 생각되면 Cisco TALOS 팀에 이의를 제출하여 수정해야 합니다.

이 작업은 다음 링크를 사용하여 수행할 수 있습니다
.https://talosintelligence.com/reputation_center/support

분쟁을 **제출하려면** 아래 지침을 따르십시오.



Lookup(조회)을 누르고 수동으로 점수를 변경하는 옵션을 입력한 후 결과가 표시됩니다.



참고: Cisco TALOS 제출은 데이터베이스에 반영되는 데 다소 시간이 걸릴 수 있습니다. 문제가 긴급한 경우 Cisco 백엔드에서 문제가 해결될 때까지 항상 **WHITELIST** 또는 **BLOCKLIST**를 작업 대상으로 생성할 수 있습니다.이를 위해 이 섹션(How To Whitelist 또는 BlackList URL)을 확인할 수 있습니다.

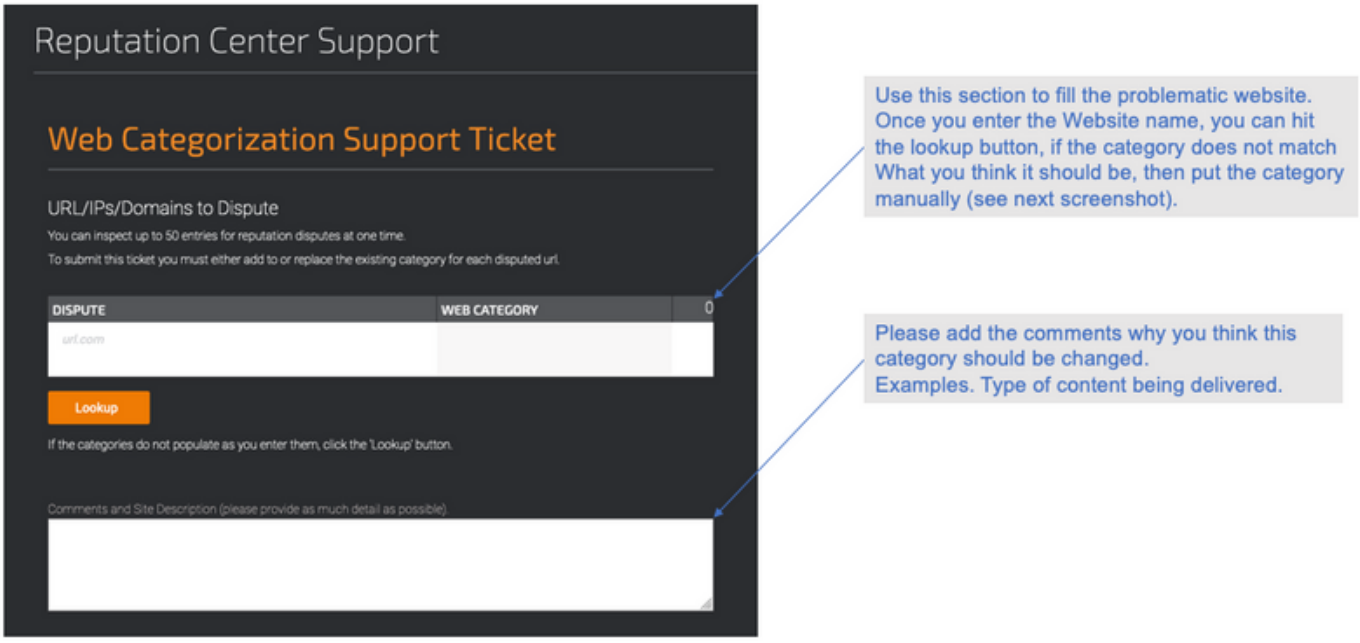
웹 평판 점수에 대한 분쟁은 어떻게 접수합니까?

Cisco WSA(Web Security Appliance)와 Cisco TALOS가 모두 동일한 범주화를 가지고 있는지 확인

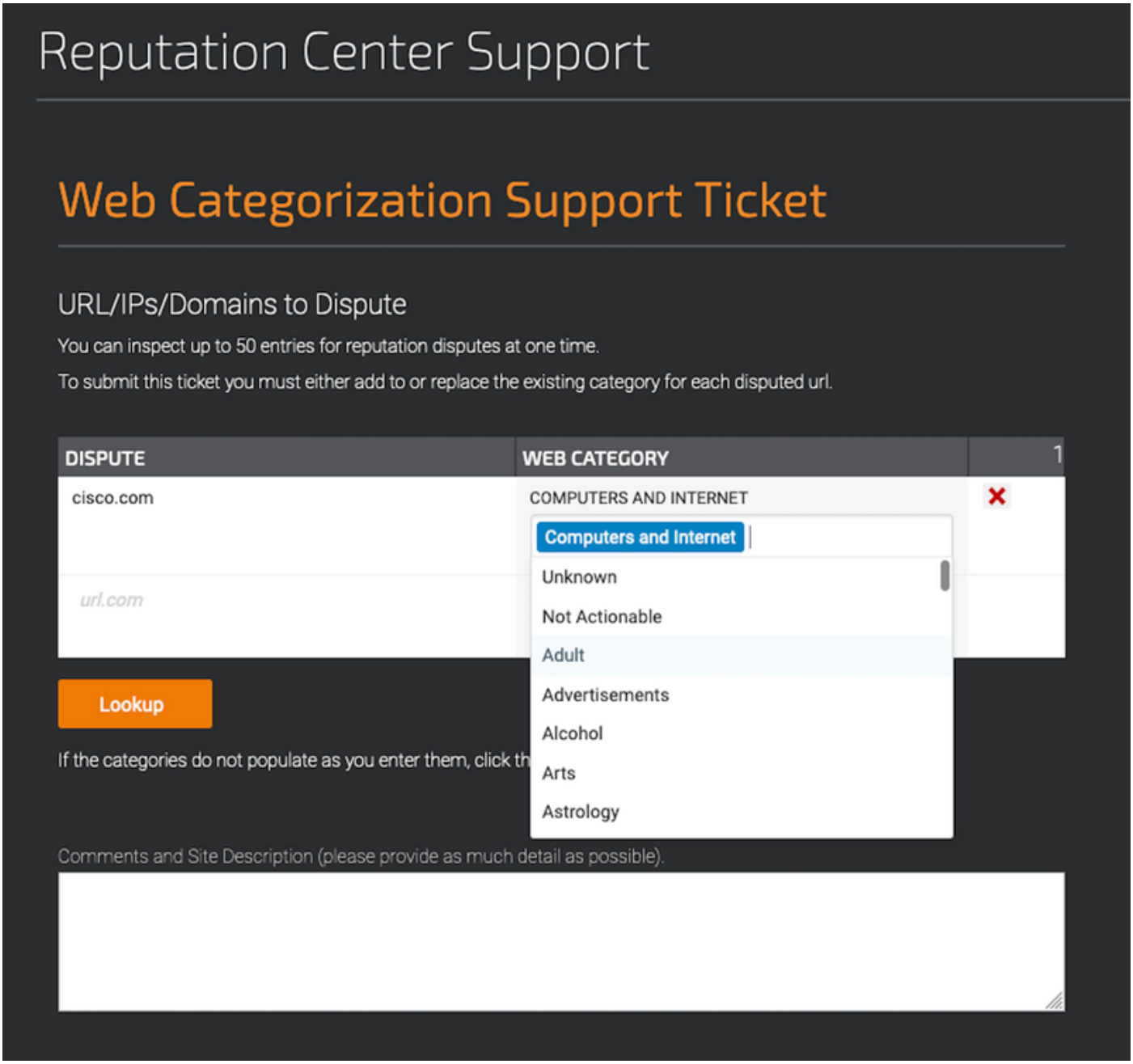
한 후에도 이 결과가 유효한 결과가 아니라고 생각되면 Cisco TALOS 팀에 이의를 제출하여 이를 해결해야 합니다.

TALOS 웹 사이트의 분류 제출 페이지로 이동합니다
.https://talosintelligence.com/reputation_center/support#categorization

분쟁을 **제출하려면** 아래 지침을 따르십시오.



카테고리를 업데이트하려면 **드롭다운** 메뉴에서 웹 사이트에 적합한 항목을 선택하고 주석 지침을 따라야 합니다.



분쟁이 발생했지만 점수 또는 범주가 Cisco WSA(Web Security Appliance) 또는 Cisco TALOS에서 업데이트되지 않았습니다.

Cisco TALOS에 케이스를 접수했으며 평판/점수가 3-4일 이내에 업데이트되지 않은 경우업데이트 설정을 확인하고 Cisco 업데이트 서버에 연결할 수 있는지 확인할 수 있습니다.이 모든 단계가 정상적으로 완료되면 Cisco TAC에서 티켓을 열고 Cisco TALOS 팀을 지원할 수 있습니다.

> **참고:**카테고리/평판이 Cisco TALOS 팀에서 업데이트될 때까지 WHITELIST/BLOCKLIST 작업을 적용하여 필요한 조치를 적용할 수 있습니다.

Cisco WSA(Web Security Appliance) Cisco TALOS와 다른 결과를 보여 주는 이 문제를 어떻게 해결할 수 있습니까?

Cisco WSA(Web Security Appliance)에서 데이터베이스가 최신 상태가 아닐 수 있는 이유는 주로

업데이트 서버와 통신하기 때문입니다. 다음 단계에 따라 정확한 업데이트 서버 및 연결을 확인하십시오.

1. 포트 80 및 443에서 Cisco 업데이트의 서버에 대한 연결이 있는지 확인합니다.

```
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. 업스트림 프록시가 있는 경우 업스트림 프록시가 업스트림 프록시를 통해 위의 테스트를 수행하는지 확인합니다.

3. 연결이 정상이지만 여전히 차이가 있는 경우 수동으로 업데이트를 강제 적용합니다.**CLI**에서 업데이트하거나 **GUI->Security services(보안 서비스) -> Malware protection -> updatenow에서 업데이트합니다**.

몇 분 정도 기다립니다. 그래도 작동하지 않으면 다음 단계를 확인하십시오.

4. 이때 updater_logs를 확인해야 합니다.열기 **터미널:CLI->tail-> (updater_logs 로그 파일 수를 선택합니다.)** 그러면 업데이트 로그에 새 라인만 표시됩니다.

로그 라인은 "Received remote **command to signal a manual update(수동 업데이트**에 **신호를 보내기 위해 원격 명령 수신)**로 시작해야 합니다.

```
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. "Critical/Warning" 메시지를 확인하고, 업데이트 로그가 사람이 읽을 수 있는 매우 오류이며, 문제가 있는 위치를 안내합니다.

6. 응답이 없는 경우 위 단계의 결과로 Cisco 지원 팀에 문의하여 티켓을 열어 주시면 기꺼이 도와드리겠습니다.

웹 평판 점수는 어떻게 계산됩니까?

특정 웹 사이트에 점수를 할당할 때 고려되는 일부 매개변수:

- URL 분류 데이터
- 다운로드 가능한 코드가 있음
- 복잡하고 긴 EULA(End-User License Agreement) 존재
- 글로벌 볼륨 및 볼륨 변경
- 네트워크 소유자 정보
- URL 기록
- URL 사용 기간
- 모든 차단 목록에 있음
- 허용 목록에 있음
- 인기 도메인의 URL 유형
- 도메인 등록자 정보
- IP 주소 정보

각 평판 범주(정상, 보통, 불량)의 점수 범위는 무엇입니까?

웹 평판 범위 및 관련 작업:

액세스 정책:

-10 ~ -6.0 ( )		. . .	• URL . • . • URL . • URL ..
-5.9 ~ 5.9 ()		. DVS . DVS .	• URL • 동적 IP 주소 및 포함 • 다운로드할 수 있습니다. • IP • 웹 평판 점수 양입니다.
6.0 ~ 10.0 ()		. . .	• URL . • • . • URL .

암호 해독 정책:

-10 ~ -9.0 ( )		. . .
-8.9 ~ 5.9 ()		. . .

6.0 ~ 10.0 ()		. .

Cisco 데이터 보안 정책:

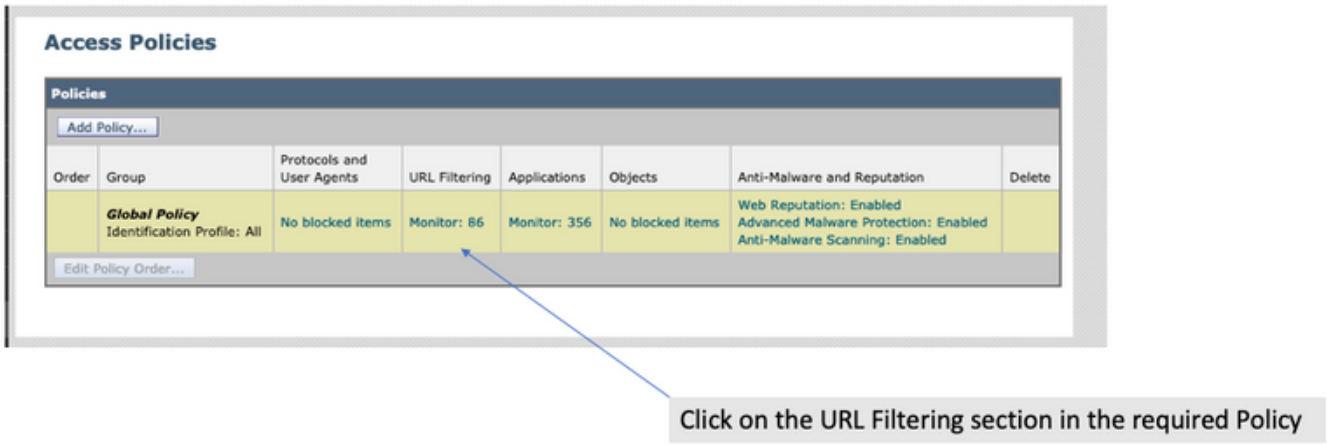
-10 ~ -6.0 ( )		. .
-5.9 ~ 0.0 ()		( ) . .

분류되지 않은 웹 사이트는 무엇을 의미합니까?

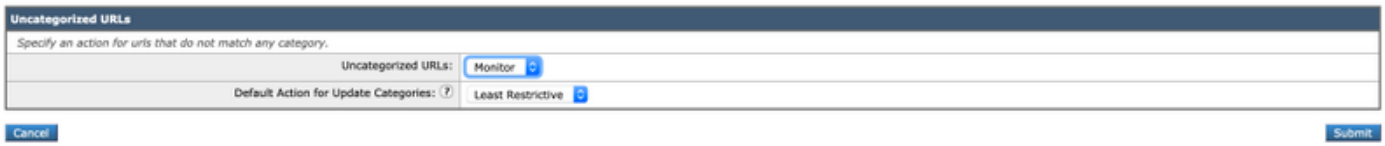
분류되지 않은 URL은 Cisco 데이터베이스에 해당 범주를 확인하는 데 필요한 정보가 충분하지 않은 URL입니다.일반적으로 새로 생성된 웹 사이트입니다.

분류되지 않은 URL을 어떻게 차단합니까?

1. 원하는 액세스 정책으로 이동합니다.**Web Security Manager -> 액세스 정책**.



2. 분류되지 않은 URLs(URL) 섹션으로 스크롤합니다.



3. 원하는 작업 중 하나, **모니터**, **차단** 또는 **경고** 중 하나를 **선택합니다**.

4. 변경 사항을 **실행하고** 커밋합니다.

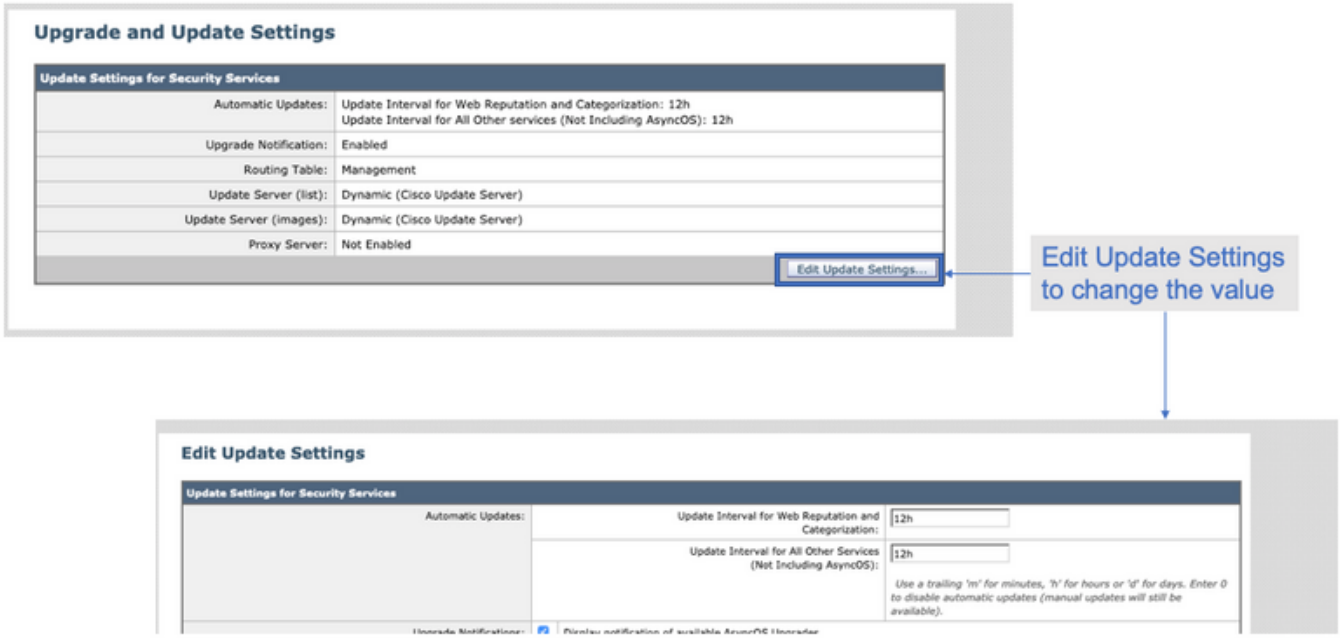
데이터베이스가 얼마나 자주 업데이트됩니까?

CLI에서 다음 명령을 사용하여 업데이트 확인 빈도를 업데이트할 수 있습니다.**업데이트 구성**

```
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
[]>
```

참고:위의 값은 업데이트를 얼마나 자주 확인하는지 보여주지만, 평판 및 기타 서비스에 대한 새 업데이트를 얼마나 자주 릴리스하는지 보여줍니다.업데이트는 언제든지 사용할 수 있습니다.

또는 GUI:**시스템 관리 -> 업그레이드 및 업데이트 설정.**



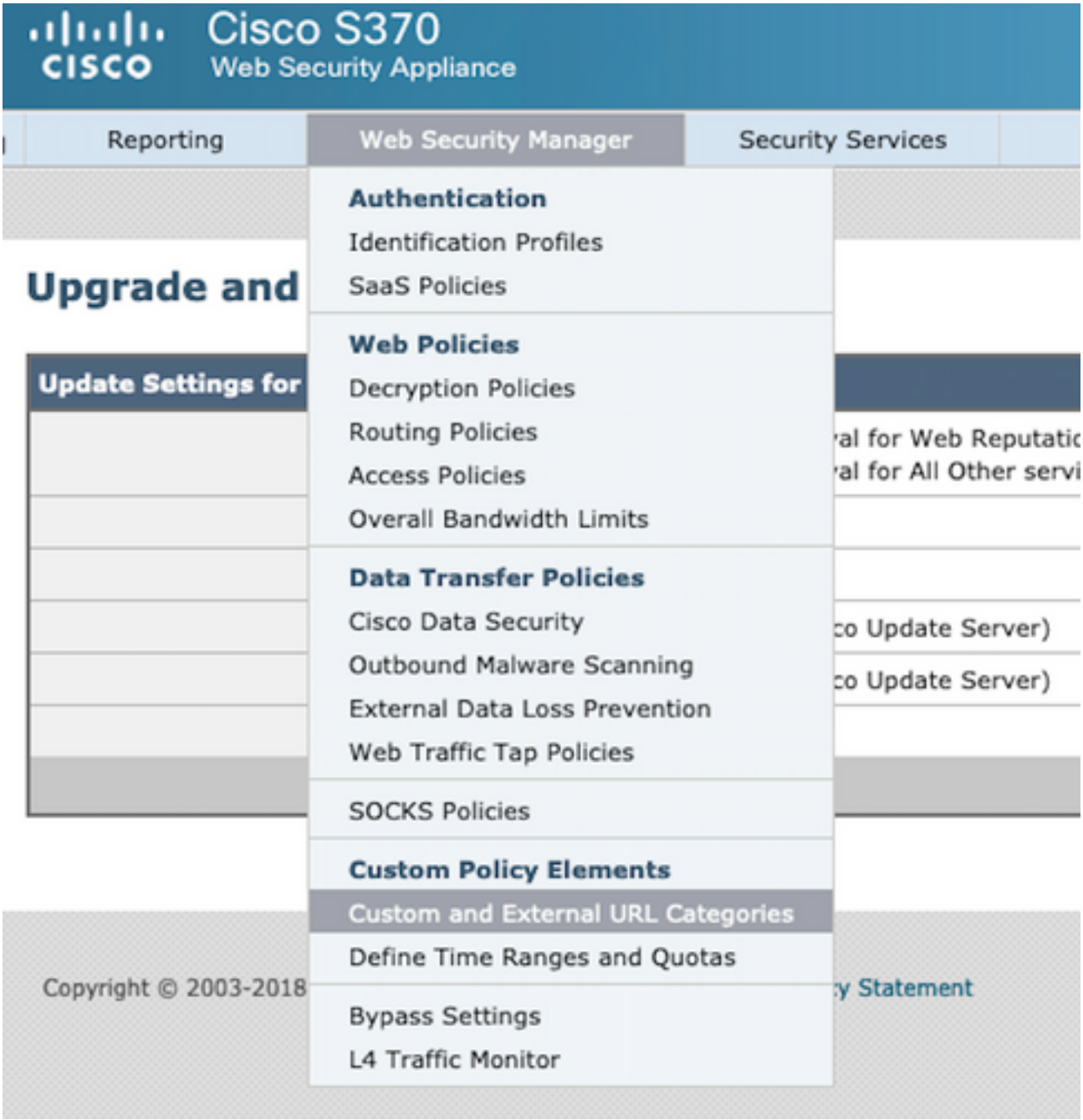
URL을 화이트리스트/블랙리스트에 추가하는 방법

Cisco TALOS에서 URL을 업데이트하는 데 시간이 걸릴 수 있습니다. 충분한 정보가 없기 때문입니다.웹 사이트가 여전히 악의적인 행동의 변화를 입증하지 못했기 때문에 평판을 바꿀 방법이 없습니다.이 시점에서 이 URL을 액세스 정책에서 허용/차단되거나 암호 해독 정책에서 통과/삭제되는 사용자 지정 URL 카테고리에 추가할 수 있으며, 그러면 Cisco WSA(Web Security Appliance) 또는 차단에서 검사 또는 URL 필터링 검사 없이 URL이 전달되도록 보장할 수 있습니다.

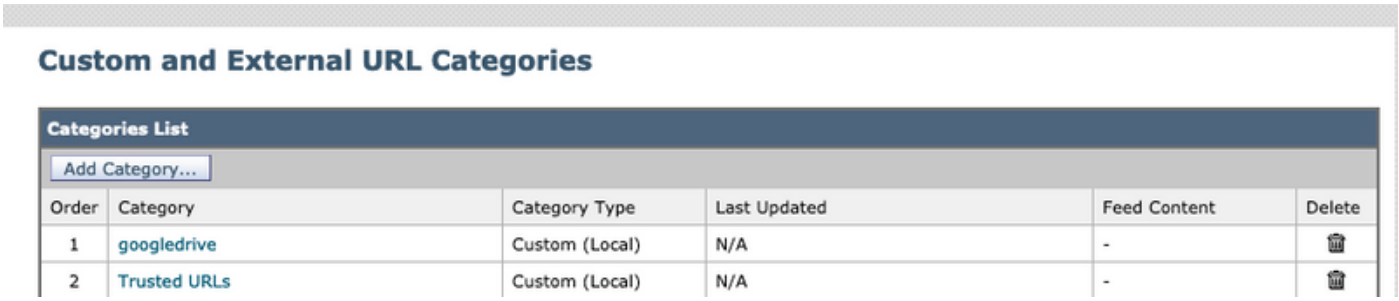
URL을 허용 목록/차단 목록에 추가하려면 다음 단계를 수행하십시오.

1. 맞춤형 URL 카테고리에 URL을 추가합니다.

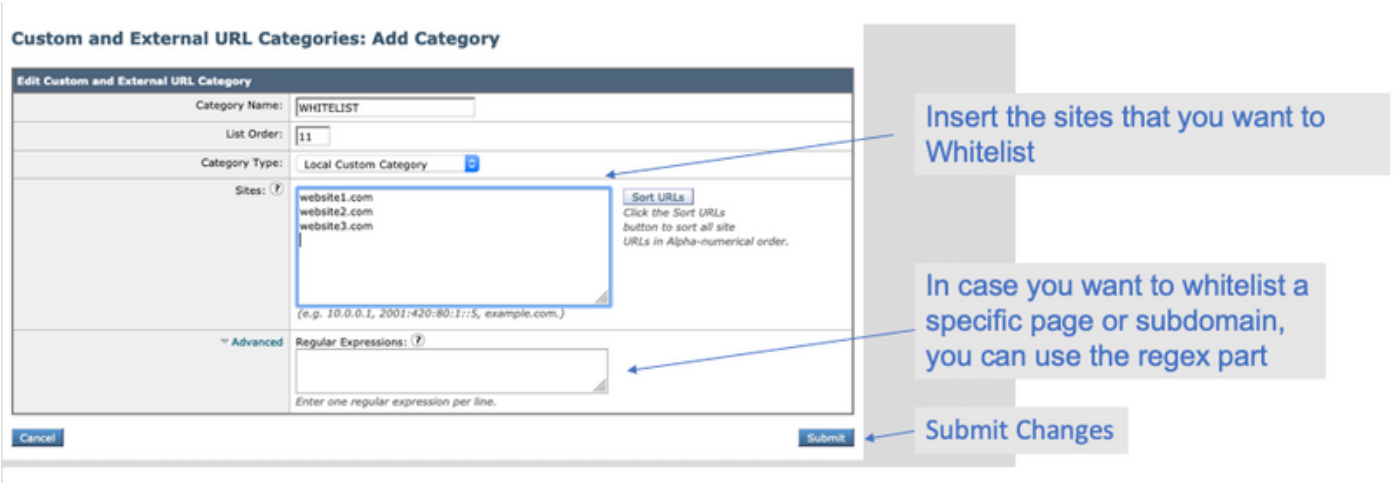
GUI에서 **Web Security Manager** -> Custom **and External URL Category로 이동합니다**.


Cisco S370
Web Security Appliance
Reporting
Web Security Manager
Security Services
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
Define Time Ranges and Quotas
Bypass Settings
L4 Traffic Monitor
Upgrade and
Update Settings for
Copyright © 2003-2018

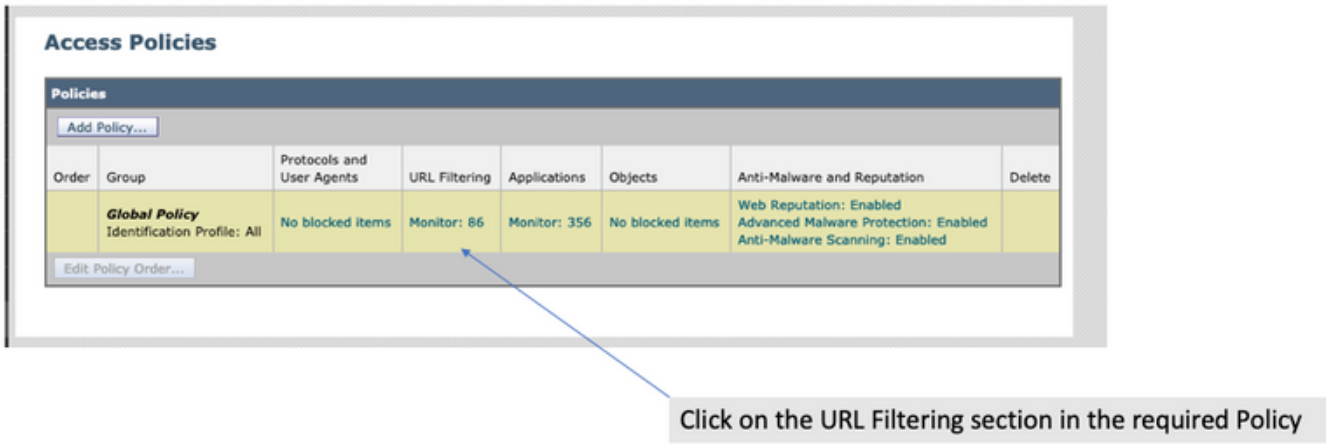
2. .


Custom and External URL Categories
Categories List
Add Category...
Order
Category
Category Type
Last Updated
Feed Content
Delete
1
googledrive
Custom (Local)
N/A
-
2
Trusted URLs
Custom (Local)
N/A
-

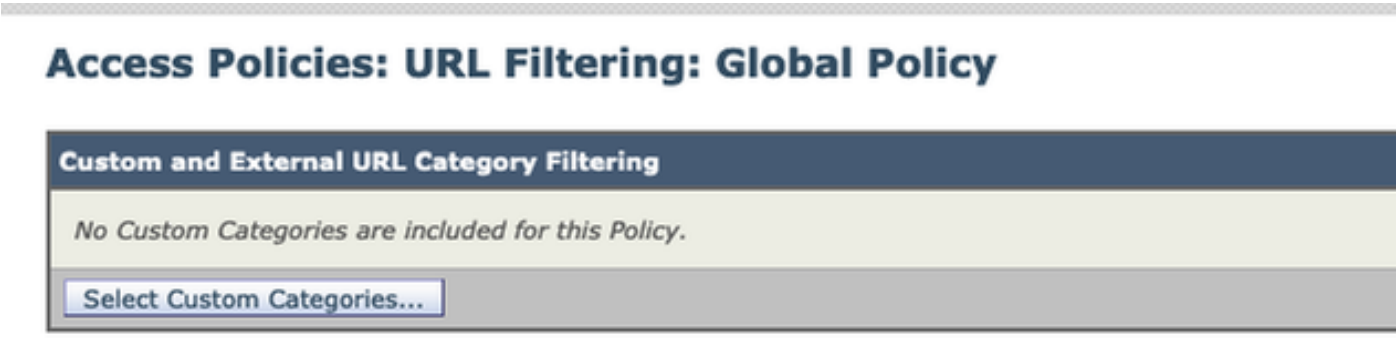
3. .



4. (**Web Security Manager -> Access Policies -> URL Filtering**) URL .

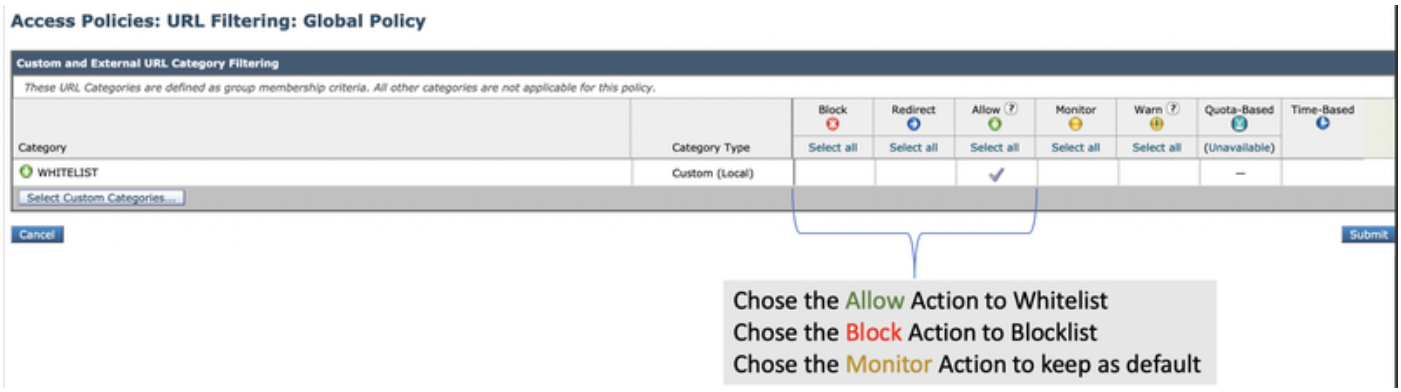


5. .



6. 다음과 같이 정책 URL 필터링 설정에 정책 범주를 포함합니다.

7. 차단 목록 차단, 허용 허용 허용 목록 작업을 정의합니다.URL이 검사 엔진을 통과하도록 하려면 Action as Monitor를 사용합니다.



8. 변경 및 **커밋**