Secure Web Appliance에서 맞춤형 URL 범주 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

맞춤형 URL 범주

라이브 피드 URL 범주

생성 단계Custom URL Categories

정규식 사용 정의

한계 및 설계 문제

정책에서 사용자 지정 URL 범주 사용

- 액세스 정책에 대한 URL 필터를 구성하는 단계
- 암호 해독 정책에 대한 URL 필터를 구성하는 단계
- 데이터 보안 정책 그룹에 대한 URL 필터를 구성하는 단계
- 맞춤형 URL 카테고리로 업로드 요청 제어를 구성하는 단계
- 외부 DLP 정책에서 ControlUpload 요청을 구성하는 단계

Bypass 및 PassthroughURL

- 웹 요청에 대한 웹 프록시 Bypass 구성

보고서

액세스 로그에서 사용자 지정 URL 범주 보기

문제 해결

- 범주가 일치하지 않음

참조

소개

이 문서에서는 SWA(Secure Web Appliance)의 사용자 지정 URL(Uniform Resource Locator) 범주 구조에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 프록시 작동 방식.
- SWA(Secure Web Appliance) 관리

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- 물리적 또는 가상 SWA(Secure Web Appliance)가 설치되었습니다.
- 라이센스가 활성화되었거나 설치되었습니다.
- 설치 마법사가 완료되었습니다.

- SWA에 대한 관리 액세스.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

맞춤형 URL 범주

URL 필터 엔진을 사용하면 액세스, 암호 해독 및 데이터 보안 정책에서 트랜잭션을 필터링할 수 있습니다. 정책 그룹에 대한 URL 카테고리를 구성할 때 맞춤형 URL 카테고리(정의된 경우) 및 사전 정의된 URL 카테고리에 대한 작업을 구성할 수 있습니다.

특정 호스트 이름 및 인터넷 프로토콜(IP) 주소를 설명하는 맞춤형 및 외부 라이브 피드 URL 카테고리를 생성할 수 있습니다. 또한 URL 카테고리를 수정하고 삭제할 수 있습니다.

동일한 액세스, 암호 해독 또는 Cisco 데이터 보안 정책 그룹에 이러한 맞춤형 URL 카테고리를 포함하고 각 카테고리에 다른 작업을 할당하면 포함된 상위 맞춤형 URL 카테고리의 작업이 우선합니다.

참고: DNS(Domain Name System)에서 웹 사이트에 대한 여러 IP를 확인하고 이러한 IP 중 하나가 사용자 지정 차단 목록이면 Web Security Appliance는 사용자 지정 차단 목록에 나열되지 않은 모든 IP에 대해 웹 사이트를 차단합니다.

라이브 피드 URL 범주

외부 라이브 피드 범주는 특정 사이트에서 URL 목록을 가져오는 데 사용됩니다. 예를 들어 Microsoft에서 Office 365 URL을 가져오는 데 사용됩니다.

사용자 지정 및 외부 URL 범주를 만들고 편집할 때 범주 유형으로 외부 라이브 피드 범주를 선택하는 경우 피드 형식(Cisco 피드 형식 또는 Office 365 피드 형식)을 선택한 다음 적절한 피드 파일 서버에 URL을 제공해야 합니다.
각 피드 파일의 예상 형식은 다음과 같습니다.

- Cisco 피드 형식 - 쉼표로 구분된 값(.csv) 파일, 즉 확장명이 .csv인 텍스트 파일이어야 합니다. .csv 파일의 각 항목은 주소/쉼표/주소 형식으로 된 별도의 줄에 있어야 합니다 (예: www.cisco.com,site 또는 ad2.*\.com,regex). 유효한 주소 유형은 사이트 및 regex입니다.

다음은 Cisco Feed Format .csv 파일의 일부입니다.

```
www.cisco.com,site
\.xyz,regex
ad2.*\.com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Office 365 피드 형식 - 파일을 저장한 Microsoft Office 365 서버 또는 로컬 서버에 있는 XML 파일입니다. Office 365 서비스에서 제공하며 수정할 수 없습니다.

파일의 네트워크 주소는 XML 태그로 둘러싸이며, 이러한 구조는 products > product > address list > address입니다. 현재 구현에서 "주소 목록 유형"은 IPv6, IPv4 또는 URL[도메인 및 정규식(regex) 패턴을 포함할 수 있음]일 수 있습니다.

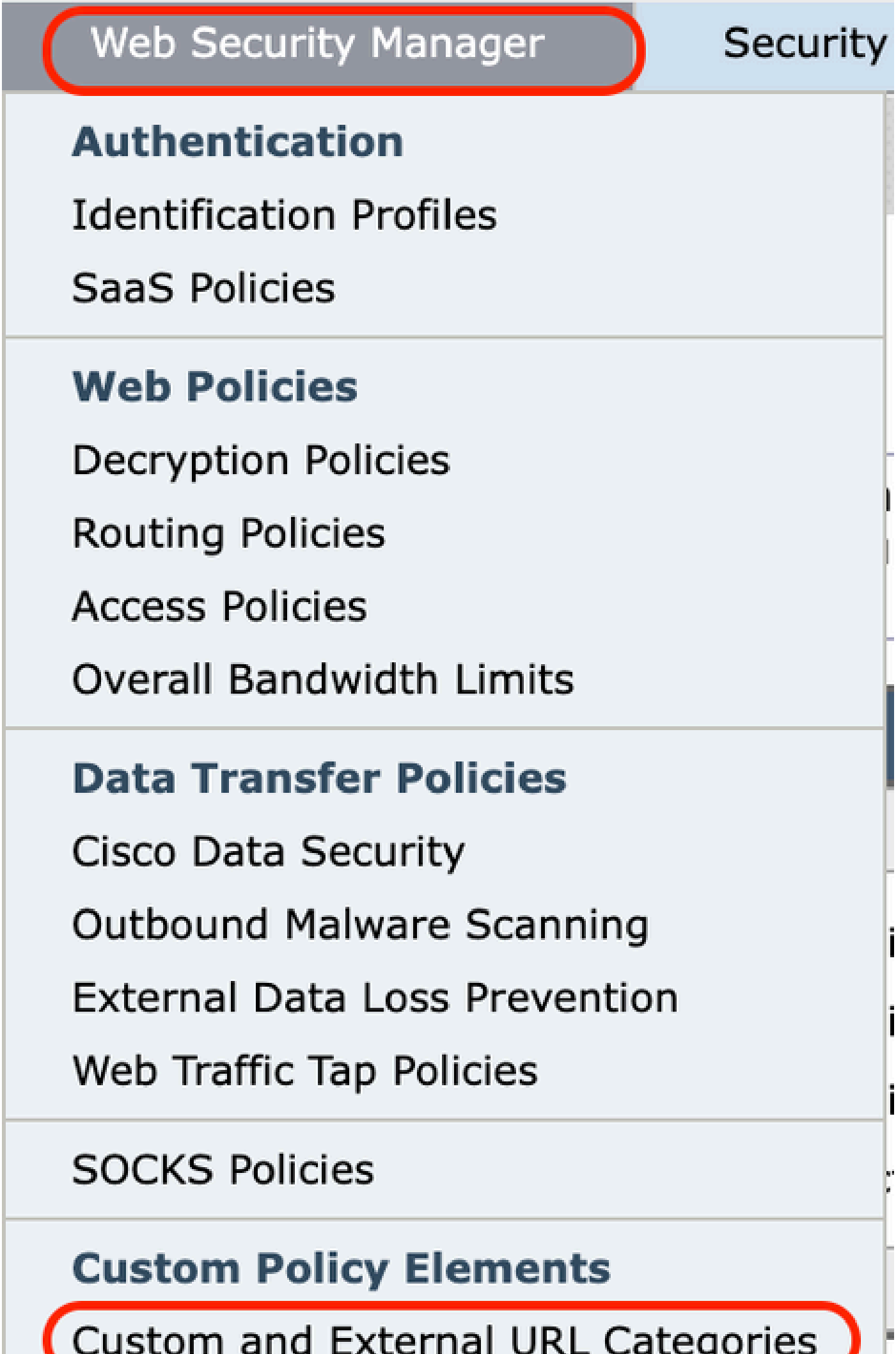
다음은 Office 365 피드 파일의 코드 조각입니다.

```
<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>
```

참고: 파일의 사이트 항목에 http:// 또는 https://을 포함시키지 마십시오. 오류가 발생합니다. 즉, www.cisco.com는 올바르게 구문 분석되지만 http://www.cisco.com은 오류를 생성합니다

맞춤형 URL 범주 생성 단계

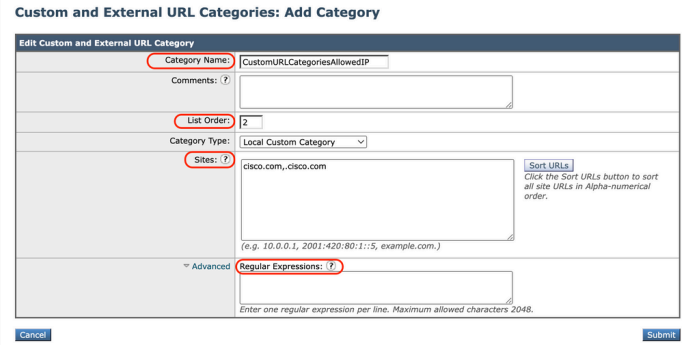
1단계. Web Security Manager(웹 보안 관리자) > Custom and External URL Categories(맞춤형 및 외부 URL 범주)를 선택합니다.

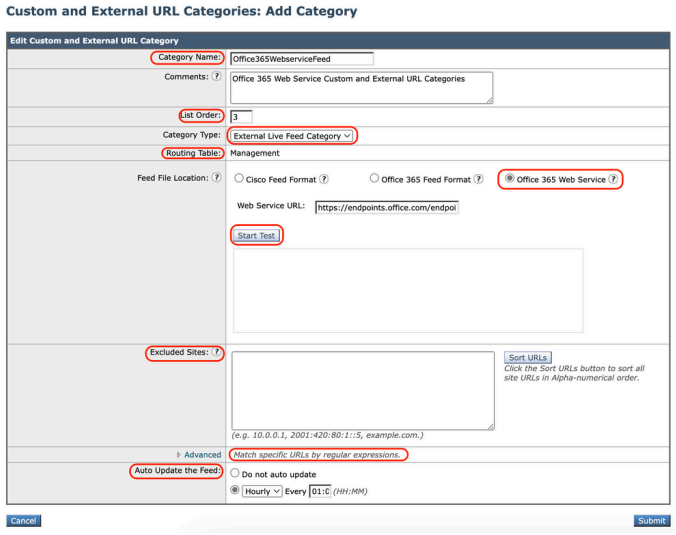

Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

URL 필터 엔진은 지정된 순서대로 맞춤형 URL 카테고리와 비교하여 클라이언트 요청을 평가합니다.

참고: URL 필터 엔진이 URL 카테고리를 클라이언트 요청의 URL과 일치시키면 먼저 정책 그룹에 포함된 맞춤형 URL 카테고리와 비교하여 URL을 평가합니다. 요청의 URL이 포함된 맞춤형 카테고리와 일치하지 않으면 URL 필터 엔진은 이를 미리 정의된 URL 카테고리와 비교합니다. URL이 포함된 맞춤형 또는 사전 정의된 URL 카테고리와 일치하지 않으면 요청이 분류되지 않습니다.

- 범주 유형: Local Custom Category(로컬 맞춤형 범주) 또는 External Live Feed Category(외부 라이브 피드 범주)를 선택합니다.
- 라우팅 테이블: 관리 또는 데이터를 선택합니다. 이 옵션은 "분할 라우팅"이 활성화된 경우에만 사용할 수 있습니다. 즉, 로컬 사용자 지정 범주에서는 사용할 수 없습니다.

<table>
<tr>
<td> 

이미지 - 로컬 맞춤형 URL 범주</td>
<td> 

이미지 - 사용자 지정 URL 범주 구성 피드</td>
</tr>
<tr>
<td>로컬 사용자 지정 범주</td>
<td>외부 라이브 피드 범주</td>
</tr>
</table>

정규식 사용 정의

Secure Web Appliance는 다른 Velocity 패턴 일치 엔진 구현에서 사용하는 정규식 구문과 약간 다른 정규식 구문을 사용합니다.

또한 어플라이언스는 슬래시를 이스케이프하는 백슬래시를 지원하지 않습니다. 정규식에서 슬래시를 사용해야 하는 경우 슬래시 없이 슬래시를 입력하면 됩니다.

참고: 기술적으로 AsyncOS for Web은 Flex 정규식 분석기를 사용합니다

정규식을 테스트하려면 다음 링크를 사용하십시오. [flex lint - Regex Tester/Debugger]

⚠ 주의: 63자 이상을 반환하는 정규식은 실패하고 잘못된 항목 오류가 발생합니다. 63자 이상을 반환할 수 있는 가능성이 없는 정규식을 구성해야 합니다.

⚠ 주의: 광범위한 문자 일치를 수행하는 정규식은 리소스를 소비하며 시스템 성능에 영향을 줄 수 있습니다. 따라서 정규식을 신중하게 적용할 수 있습니다.

다음 위치에서 정규식을 사용할 수 있습니다.
· 액세스 정책에 대한 맞춤형 URL 카테고리 액세스 정책 그룹과 함께 사용할 사용자 지정 URL 카테고리를 만들 때 정규식을 사용하여 입력한 패턴과 일치하는 여러 웹 서버를 지정할 수 있습니다.
· 차단할 사용자 지정 사용자 에이전트 액세스 정책 그룹에 대해 차단할 애플리케이션을 편집할 때 정규식을 사용하여 차단할 특정 사용자 에이전트를 입력할 수 있습니다.

팁: 정규식에 대한 웹 프록시 우회를 설정할 수 없습니다.

다음은 Flex 정규식의 문자 클래스 목록입니다.

문자 클래스	
.	줄 바꿈을 제외한 모든 문자
\w \d \s	단어, 숫자, 공백
\W \D \S	단어, 숫자, 공백 아님
[abc]	a, b 또는 c 중 하나
[^abc]	a, b 또는 c가 아님
[a-g]	a와 g 사이의 문자
앵커	
^abc$	문자열의 시작/끝
\b	단어 경계
이스케이프된 문자	
\. * \\	이스케이프된 특수 문자
\t \n \r	tab, linefeed, 캐리지 리턴
A9	유니코드 이스케이프된 ©
그룹 및 둘러보기	
(abc)	캡처 그룹
\1	그룹 정책에 대한 역참조 #1
(?:abc)	비포획 그룹
(?=abc)	긍정적인 전망
(?!abc)	부정적인 향후 전망
수량자 및 대안	
a* a+ a?	0 이상, 1 이상, 0 또는 1
a{5} a{2,}	정확히 5개, 2개 또는 그 이상

a{1,3}	1~3개
a+? a{2,}?	가능한 한 적게 일치
ab|cd	ab 또는 cd 일치

⚠ 주의: 긴 패턴의 이스케이프되지 않은 점, 특히 긴 패턴의 중간에 있는 점을 경계하고 특히 점 문자와 함께 이 메타 문자(Star *)를 경계합니다. 모든 패턴에는 이스케이프되지 않은 점이 포함되어 있으며, 점이 비활성화된 후 63자 이상을 반환합니다.
항상 이스케이프 *(별표) 및 . (점) \ (백슬래시)가 있는 경우(예: * 및 \).
정규식에서 .cisco.local을 사용하는 경우 Xcisco.local 도메인도 일치합니다.
이스케이프되지 않은 문자는 성능에 영향을 미치며 웹 브라우징 중에 속도가 느려집니다. 이는 패턴 일치 엔진이 올바른 항목에 대한 일치 항목을 찾을 때까지 수천 또는 수백만 개의 가능성을 검토해야 하기 때문입니다. 또한 허용된 정책의 유사 URL과 관련하여 몇 가지 보안 문제가 있을 수 있습니다

CLI(command-line interface) 옵션 advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex, to enable or disable default regex conversion to lower case-insensitive matches를 사용할 수 있습니다. 대/소문자를 구분하는 데 문제가 있는 경우 사용합니다.

한계 및 설계 문제

- 이러한 URL 범주 정의에 외부 라이브 피드 파일을 30개 이하로 사용할 수 있으며 각 파일에는 5000개 이하의 항목이 포함되어야 합니다.
- 외부 피드 항목 수가 증가하면 성능 저하가 발생합니다.
- 여러 맞춤형 URL 카테고리에서 동일한 주소를 사용할 수 있지만 카테고리가 나열되는 순서는 관련이 있습니다.

이러한 카테고리를 동일한 정책에 포함하고 각각에 대해 서로 다른 작업을 정의하는 경우 맞춤형 URL 카테고리 테이블에 가장 높게 나열된 카테고리에 대해 정의된 작업이 적용됩니다.

- 네이티브 FTP(File Transfer Protocol) 요청이 FTP 프록시에 투명하게 리디렉션되는 경우 FTP 서버에 대한 호스트 이름 정보가 없고 IP 주소만 포함합니다.

이 때문에 호스트 이름 정보만 있는 일부 사전 정의된 URL 범주 및 웹 평판 필터는 요청이 해당 서버로 향하는 경우에도 네이티브 FTP 요청과 일치하지 않습니다.

이러한 사이트에 대한 액세스를 차단하려면 해당 IP 주소를 사용할 맞춤형 URL 카테고리를 생성해야 합니다.

- 분류되지 않은 URL은 미리 정의된 URL 카테고리 또는 포함된 맞춤형 URL 카테고리와 일치하지 않는 URL입니다

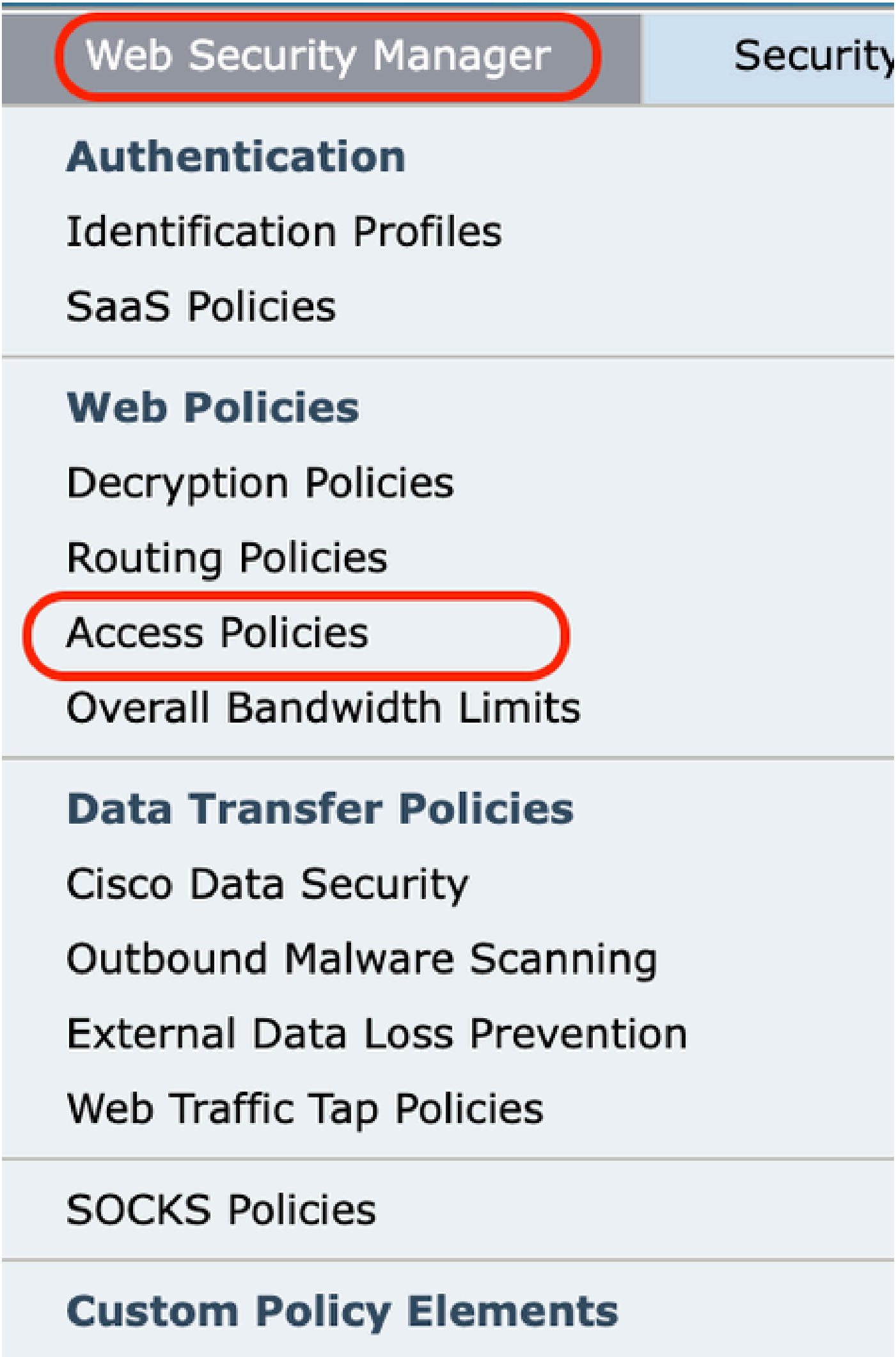
정책에서 사용자 지정 URL 범주 사용

URL 필터 엔진을 사용하면 액세스, 암호 해독 및 데이터 보안 정책에서 트랜잭션을 필터링할 수 있습니다. 정책 그룹에 대한 URL 카테고리를 구성할 때 맞춤형 URL 카테고리(정의된 경우) 및 사전

정의된 URL 카테고리에 대한 작업을 구성할 수 있습니다.

액세스 정책에 대한 URL 필터를 구성하는 단계

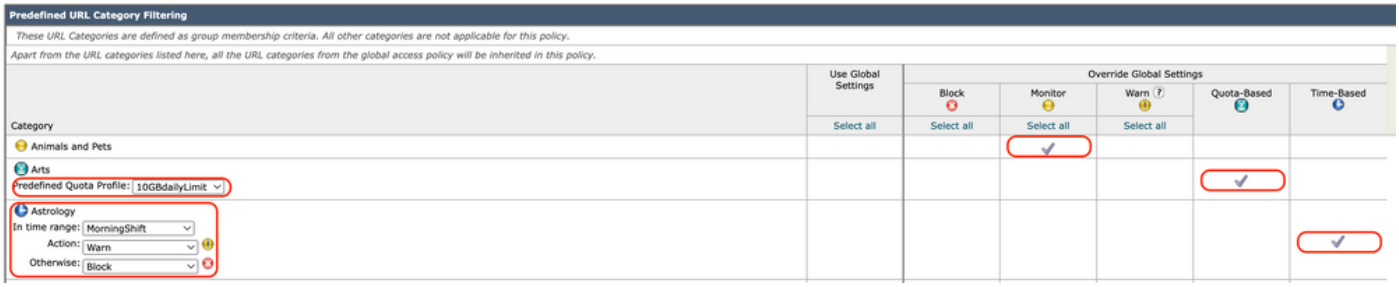
1단계. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)를 선택합니다.


Web Security Manager
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

작업	설명
차단	웹 프록시는 이 설정과 일치하는 트랜잭션을 거부합니다.
리디렉션	원래 이 카테고리의 URL로 지정된 트래픽을 사용자가 지정한 위치로 리디렉션합니다. 이 작업을 선택하면 Redirect To(리디렉션 대상) 필드가 나타납니다. 모든 트래픽을 리디렉션할 URL을 입력합니다.
허용	이 범주의 웹 사이트에 대한 클라이언트 요청을 항상 허용합니다. 허용된 요청은 모든 추가 필터 및 악성코드 스캔을 우회합니다. 신뢰할 수 있는 웹 사이트에만 이 설정을 사용합니다. 내부 사이트에 이 설정을 사용할 수 있습니다.
모니터링	웹 프록시는 요청을 허용하거나 차단하지 않습니다. 대신, 웹 평판 필터와 같은 다른 정책 그룹 제어 설정과 비교하여 클라이언트 요청을 계속 평가합니다.
경고	웹 프록시는 처음에 요청을 차단하고 경고 페이지를 표시하지만 사용자가 경고 페이지에서 하이퍼텍스트 링크를 클릭하여 계속할 수 있도록 합니다.
할당량 기반	개별 사용자가 지정한 볼륨 또는 시간 할당량에 접근하면 경고가 표시됩니다. 할당량이 충족되면 차단 페이지가 표시됩니다. .
시간 기반	웹 프록시는 사용자가 지정한 시간 범위 동안 요청을 차단하거나 모니터링합니다.

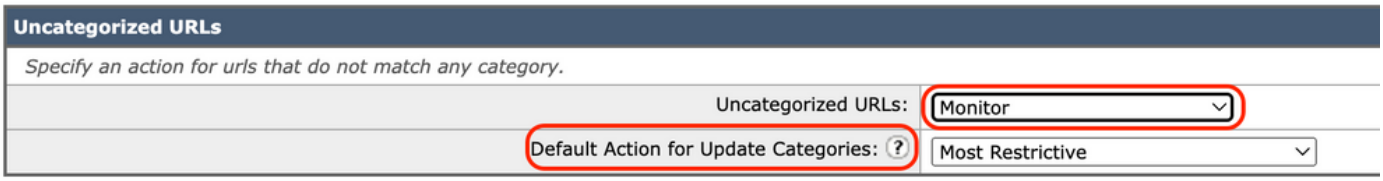
5단계. Predefined URL Category Filter(사전 정의된 URL 카테고리 필터) 섹션에서 각 카테고리에 대해 다음 작업 중 하나를 선택합니다.

- 전역 설정 사용
- 모니터링
- 경고
- 차단
- 시간 기반
- 할당량 기반



Image(이미지) - 미리 정의된 카테고리에 대한 Action(작업)을 선택합니다.

6단계. Uncategorized URLs(분류되지 않은 URL) 섹션에서 사전 정의 또는 사용자 지정 URL 카테고리에 속하지 않는 웹 사이트에 대한 클라이언트 요청에 대해 수행할 작업을 선택합니다. 이 설정은 또한 URL 범주 집합 업데이트에서 새 범주와 병합된 범주의 기본 작업을 결정합니다.

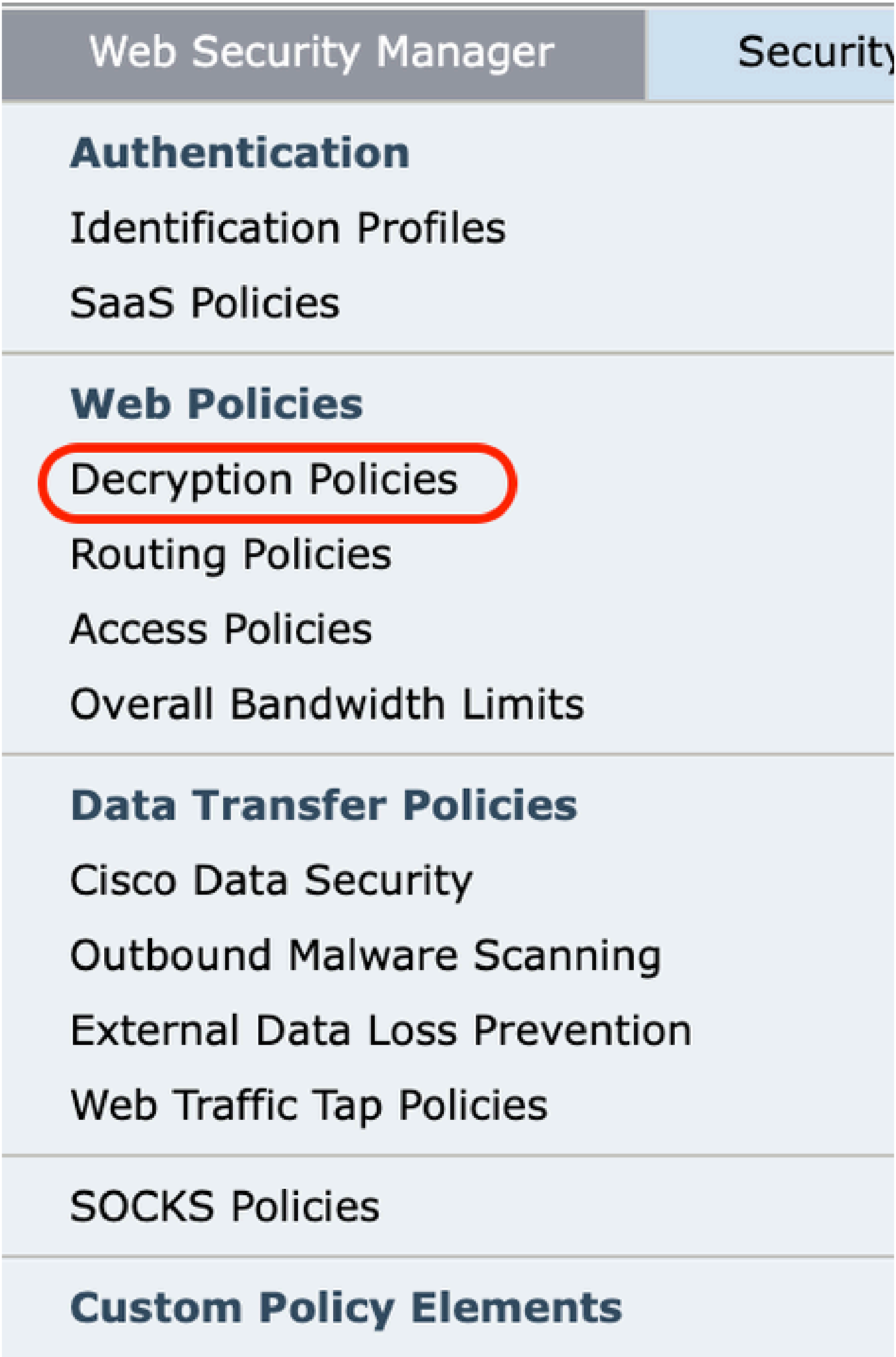


Image(이미지) - 분류되지 않은 URL에 대한 작업을 선택합니다.

7단계. 변경 사항을 제출 및 커밋합니다.

암호 해독 정책에 대한 URL 필터를 구성하는 단계

1단계. Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책)를 선택합니다.


Web Security Manager
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

작업	설명
	카테고리가 전역 암호 해독 정책에서 제외되는 경우 사용자 정의 암호 해독 정책에 포함된 사용자 지정 URL 카테고리에 대한 기본 작업은 Use Global Settings(전역 설정 사용) 대신 Monitor(모니터링)입니다. 맞춤형 URL 카테고리가 전역 암호 해독 정책에서 제외된 경우 Use Global Settings(전역 설정 사용)를 선택할 수 없습니다.
통과	트래픽 콘텐츠를 검사하지 않고 클라이언트와 서버 간의 연결을 통과합니다.
모니터링	웹 프록시는 요청을 허용하거나 차단하지 않습니다. 대신, 웹 평판 필터와 같은 다른 정책 그룹 제어 설정과 비교하여 클라이언트 요청을 계속 평가합니다.
암호 해독	연결을 허용하지만 트래픽 콘텐츠를 검사합니다. 어플라이언스는 트래픽을 해독하고 해독된 트래픽에 액세스 정책을 일반 텍스트 HTTP(Hypertext Transfer Protocol) 연결인 것처럼 적용합니다. 연결이 해독되고 액세스 정책이 적용되면 트래픽에서 악성코드를 스캔할 수 있습니다.
삭제	연결을 삭제하고 서버에 연결 요청을 전달하지 않습니다. 어플라이언스는 사용자에게 연결을 삭제했음을 알리지 않습니다.

5단계. Uncategorized URLs(분류되지 않은 URL) 섹션에서 사전 정의 또는 사용자 지정 URL 카테고리에 속하지 않는 웹 사이트에 대한 클라이언트 요청에 대해 수행할 작업을 선택합니다.

이 설정은 또한 URL 범주 집합 업데이트에서 새 범주와 병합된 범주의 기본 작업을 결정합니다.

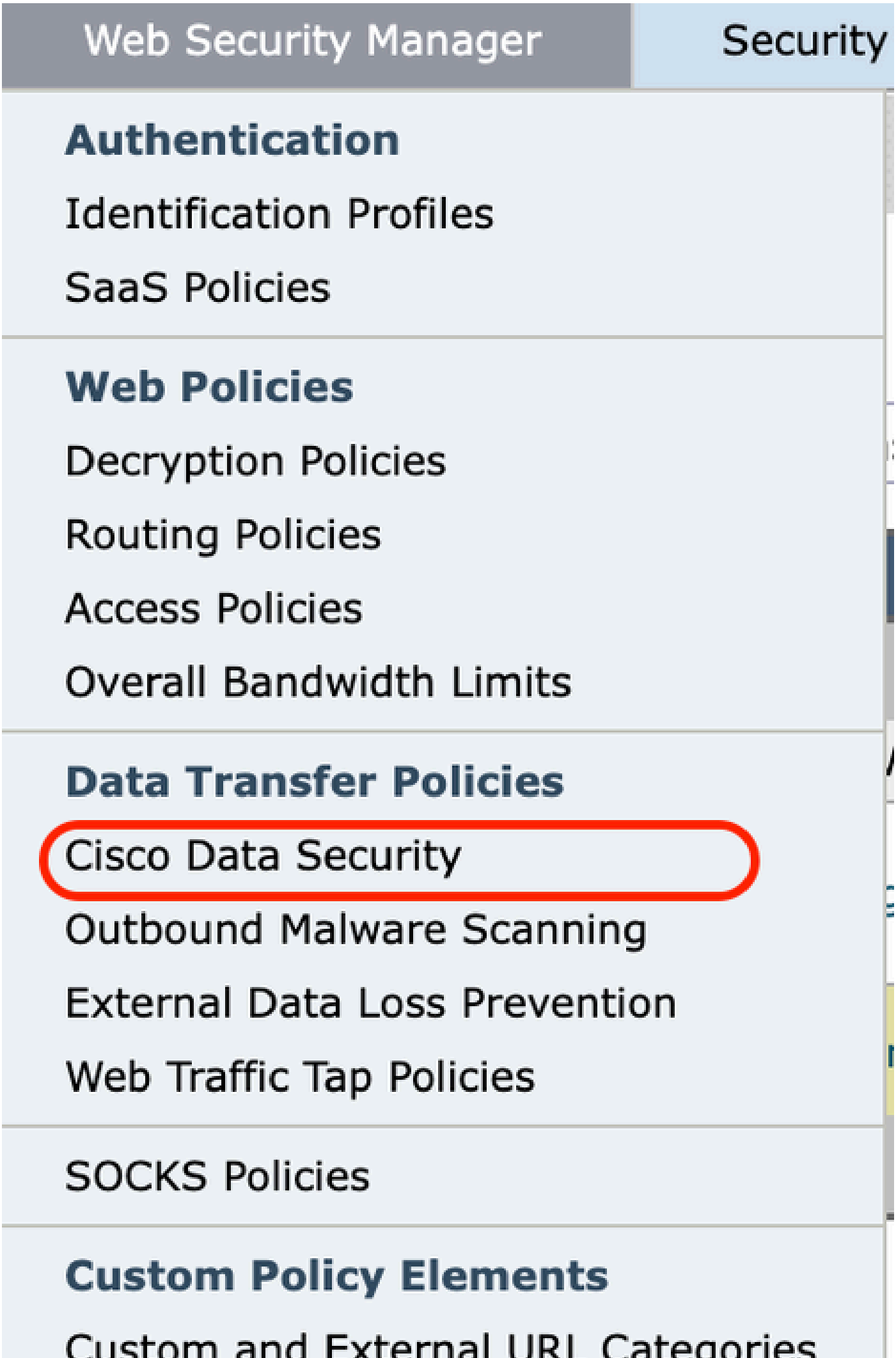
이미지 - 분류되지 않은 암호 해독 정책

6단계. 변경 사항을 제출 및 커밋합니다.

⚠ 주의: HTTPS(Hypertext Transfer Protocol Secure) 요청에 대한 특정 URL 카테고리를 차단하려면 암호 해독 정책 그룹에서 해당 URL 카테고리의 암호를 해독하도록 선택한 다음 액세스 정책 그룹에서 동일한 URL 카테고리를 차단하도록 선택합니다.

데이터 보안 정책 그룹에 대한 URL 필터를 구성하는 단계

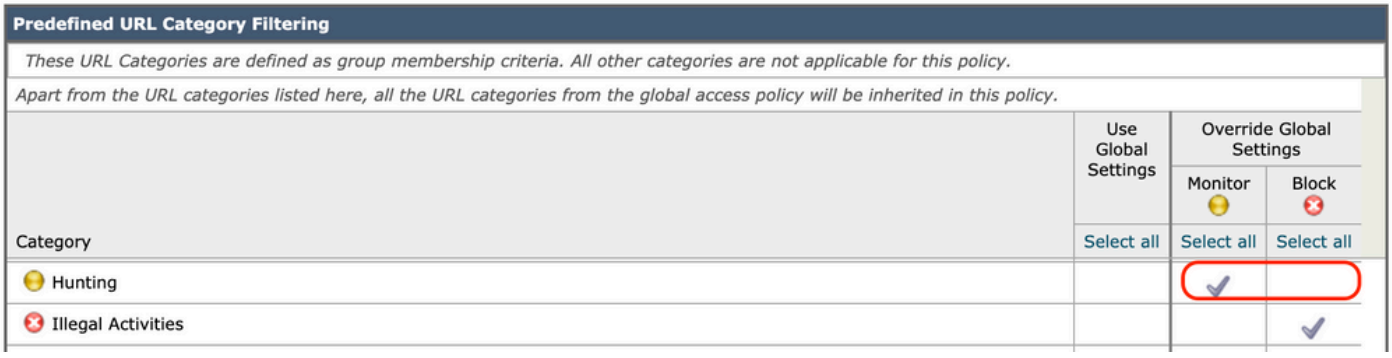
1단계. Web Security Manager(웹 보안 관리자) > Cisco Data Security를 선택합니다.


Web Security Manager
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

작업	설명
허용	이 범주의 웹 사이트에 대한 업로드 요청을 항상 허용합니다. 맞춤형 URL 카테고리에만 적용됩니다. 허용된 요청은 모든 추가 데이터 보안 스캔을 우회하며, 요청은 액세스 정책과 비교하여 평가됩니다. 신뢰할 수 있는 웹 사이트에만 이 설정을 사용합니다. 내부 사이트에 이 설정을 사용할 수 있습니다.
모니터링	웹 프록시는 요청을 허용하거나 차단하지 않습니다. 그 대신, 웹 평판 필터와 같은 다른 정책 그룹 제어 설정에 대해 업로드 요청을 계속 평가합니다.
차단	웹 프록시는 이 설정과 일치하는 트랜잭션을 거부합니다.

5단계. Predefined URL Category Filtering(미리 정의된 URL 카테고리 필터링) 섹션에서 각 카테고리에 대해 다음 작업 중 하나를 선택합니다.

- 전역 설정 사용
- 모니터링
- 차단



이미지 - 데이터 보안 사전 정의된 URL 작업 선택

6단계. Uncategorized URLs(분류되지 않은 URL) 섹션에서 미리 정의된 또는 맞춤형 URL 카테고리에 속하지 않는 웹 사이트에 대한 업로드 요청에 대해 수행할 작업을 선택합니다.

이 설정은 또한 URL 범주 집합 업데이트에서 새 범주와 병합된 범주의 기본 작업을 결정합니다.

7단계. 변경 사항을 제출 및 커밋합니다.

⚠ 주의: 최대 파일 크기 제한을 비활성화하지 않으면 URL 필터링에서 Allow(허용) 또는 Monitor(모니터링) 옵션이 선택된 경우 Web Security Appliance에서 계속해서 최대 파일 크기를 검증합니다.

맞춤형 URL 카테고리로 업로드 요청 제어를 구성하는 단계

각 업로드 요청은 "아웃바운드 악성코드 스캐닝" 정책 그룹에 할당되며 해당 정책 그룹의 제어 설정을 상속합니다.

웹 프록시가 업로드 요청 헤더를 수신하면 요청 본문을 스캔해야 하는지 여부를 결정하는 데 필요한 정보를 포함합니다.

DVS 엔진이 요청을 검사하고 웹 프록시에 판정을 반환합니다. 해당하는 경우 최종 사용자에게 차단 페이지가 나타납니다.

<table>
<tr><td>1단계</td><td>Web Security Manager(웹 보안 관리자) > Outbound Malware Scanning(아웃바운드 악성코드 스캐닝)을 선택합니다.</td></tr>
<tr><td>2단계</td><td>Destinations(대상) 열에서 구성하려는 정책 그룹에 대한 링크를 클릭합니다.</td></tr>
<tr><td>3단계</td><td>Edit Destination Settings(대상 설정 편집) 섹션의 드롭다운 메뉴에서 "Define Destinations Scanning Custom Settings(대상 스캐닝 맞춤형 설정 정의)"를 선택합니다.</td></tr>
<tr><td>4단계</td><td>Destinations to Scan(검사할 대상) 섹션에서 다음 중 하나를 선택합니다.
<table>
<tr><th>옵션</th><th>설명</th></tr>
<tr><td>업로드를 검사하지 않음</td><td>DVS 엔진이 업로드 요청을 검사하지 않습니다. 모든 업로드 요청은 액세스 정책과 비교하여 평가됩니다</td></tr>
<tr><td>모든 업로드 검사</td><td>DVS 엔진이 모든 업로드 요청을 검사합니다. 업로드 요청은 DVS 엔진 스캔 판정에 따라 액세스 정책에 대해 차단되거나 평가됩니다</td></tr>
<tr><td>지정된 사용자 지정</td><td>DVS 엔진은 특정 맞춤형 URL 카테고리에 속하는 업로드 요청을</td></tr>
</table>
</td></tr>
</table>

	옵션	설명
	URL 범주에 대한 업로드 검사	스캔합니다. 업로드 요청은 DVS 엔진 스캔 판정에 따라 액세스 정책에 대해 차단되거나 평가됩니다. Edit custom categories list(맞춤형 카테고리 목록 수정)를 클릭하여 검사할 URL 카테고리를 선택합니다
5단계	변경 사항을 제출합니다.	
6단계	Anti-Malware Filtering 열에서 정책 그룹에 대한 링크를 클릭합니다.	
7단계	Anti-Malware Settings(안티멀웨어 설정) 섹션에서 Define Anti-Malware Custom Settings(안티멀웨어 맞춤형 설정 정의)를 선택합니다.	
8단계	Cisco DVS Anti-Malware Settings(Cisco DVS 안티멀웨어 설정) 섹션에서 이 정책 그룹에 대해 활성화할 안티멀웨어 스캔 엔진을 선택합니다.	
9단계	Malware Categories(악성코드 카테고리) 섹션에서 다양한 악성코드 카테고리를 모니터링할지 차단할지를 선택합니다. 이 섹션에 나열된 카테고리는 활성화하는 스캔 엔진에 따라 다릅니다.	
10단계	변경 사항을 제출 및 커밋합니다.	

외부 DLP 정책에서 제어 업로드 요청을 구성하는 단계

웹 프록시가 업로드 요청 헤더를 수신하면 요청이 검사를 위해 외부 DLP 시스템으로 이동할 수 있는지 여부를 결정하는 데 필요한 정보가 포함됩니다.

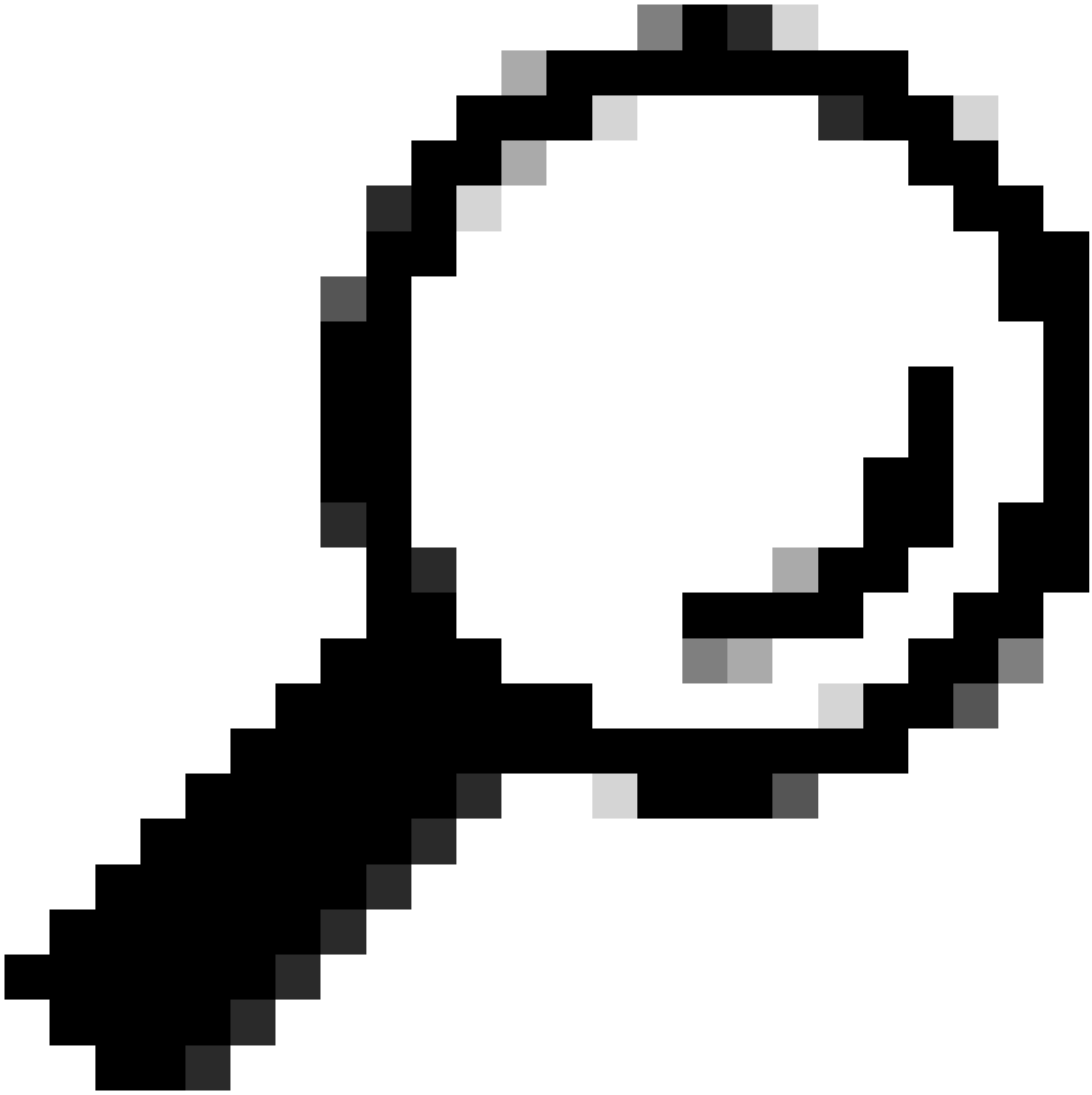
DLP 시스템은 요청을 검사하고 차단 또는 모니터링(액세스 정책과 비교하여 요청 평가)을 통해 웹 프록시에 판정을 반환합니다.

1단계	Web Security Manager > External Data Loss Prevention을 선택합니다.
2단계	구성할 정책 그룹에 대한 Destinations(대상) 열 아래의 링크를 클릭합니다.

3단계	Edit Destination Settings(대상 설정 편집) 섹션에서 "Define Destinations Scanning Custom Settings(대상 스캐닝 맞춤형 설정 정의)"를 선택합니다.
4단계	Destination to scan(스캔할 대상) 섹션에서 다음 옵션 중 하나를 선택합니다. • 업로드를 검사하지 마십시오. 구성된 DLP(Data Loss Prevention) 시스템에 검사를 위해 업로드 요청이 전송되지 않습니다. 모든 업로드 요청은 액세스 정책과 비교하여 평가됩니다. • 모든 업로드를 검사합니다. 모든 업로드 요청은 검사를 위해 구성된 DLP 시스템으로 전송됩니다. 업로드 요청은 DLP 시스템 검사 판정에 따라 액세스 정책에 대해 차단되거나 평가됩니다. • 지정된 맞춤형 및 외부 URL 카테고리를 제외한 업로드를 검사합니다. 특정 맞춤형 URL 카테고리에 속하는 업로드 요청은 DLP 스캔 정책에서 제외됩니다. 검사할 URL 범주를 선택하려면 Edit custom categories list를 클릭합니다.
5단계	변경 사항을 제출 및 커밋합니다.

Bypass 및 Passthrough URL

특정 클라이언트 또는 특정 대상에서 HTTP 또는 HTTPS 요청을 우회하도록 투명 프록시 구현의 Secure Web Appliance를 구성할 수 있습니다.



팁: 대상 서버의 수정 또는 인증서 확인 없이 어플라이언스를 통과하는 트래픽이 필요한 애플리케이션에 패스스루를 사용할 수 있습니다

⚠ 주의: 도메인 맵 기능은 HTTPS 투명 모드에서 작동합니다. 이 기능은 명시적 모드 및 HTTP 트래픽에서 작동하지 않습니다.

- 트래픽이 이 기능을 사용할 수 있도록 로컬 맞춤형 카테고리를 구성해야 합니다.
- 이 기능을 활성화하면 SNI(Server Name Indication) 정보를 사용할 수 있는 경우에도 도메인 맵에 구성된 서버 이름에 따라 서버 이름을 수정하거나 할당합니다.
- 이 기능은 도메인 이름을 기준으로 트래픽이 도메인 맵과 일치하고 사용자 지정 카테고리, 암호 해독 정책 및 통과 작업이 구성된 경우 트래픽을 차단하지 않습니다.

- 이 통과 기능에서는 인증이 작동하지 않습니다. 인증에는 암호 해독이 필요하지만 이 경우 트래픽은 암호 해독되지 않습니다.
- 트래픽은 모니터링되지 않습니다. Web Security Appliance에 도달하지 않도록 UDP 트래픽을 구성해야 합니다. 대신 WhatsApp, Telegram 등의 애플리케이션을 위해 방화벽을 통해 인터넷으로 직접 이동해야 합니다.
- WhatsApp, Telegram 및 Skype는 투명 모드에서 작동합니다. 다만 왓츠앱과 같은 일부 앱은 앱의 제한 때문에 명시적 모드에서 작동하지 않는다.

특정 서버에 대한 통과 트래픽이 필요한 디바이스에 대해 식별 정책을 정의했는지 확인합니다. 특히 다음을 수행해야 합니다.

- 인증/식별에서 제외를 선택합니다.
- 이 식별 프로필을 적용해야 하는 주소를 지정합니다. IP 주소, CIDR(Classless Inter-Domain Routing) 블록 및 서브넷을 사용할 수 있습니다.

<table>
<tr><td>1단계</td><td>HTTPS 프록시를 활성화합니다.</td></tr>
<tr><td>2단계</td><td>Web Security Manager > Domain Map을 선택합니다.
a. Add Domain(도메인 추가)을 선택합니다.
b. 도메인 이름 또는 대상 서버를 입력합니다.
c. 일부 도메인이 지정된 경우 우선순위의 순서를 선택합니다.
d. IP 주소를 입력합니다.
e. Submit(제출)을 클릭합니다.</td></tr>
<tr><td>3단계</td><td>Web Security Manager > Custom and External URL Categories를 선택합니다.
a. Add Category를 선택합니다.
b. 이러한 정보를 제공합니다.<table><tr><th>설정</th><th>설명</th></tr><tr><td>범주 이름</td><td>이 URL 카테고리의 식별자를 입력합니다. 이 이름은 정책 그룹에 대한 URL 필터를 구성할 때 나타납니다.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>설정</th><th>설명</th></tr>
<tr><td>목록 순서</td><td>사용자 지정 URL 범주 목록에서 이 범주의 순서를 지정합니다. 목록의 첫 번째 URL 카테고리에 "1"을 입력합니다.

URL 필터 엔진은 지정된 순서대로 맞춤형 URL 카테고리와 비교하여 클라이언트 요청을 평가합니다.</td></tr>
<tr><td>범주 유형</td><td>Local Custom Category(로컬 맞춤형 범주)를 선택합니다.</td></tr>
<tr><td>고급</td><td>추가 주소 집합을 지정하려면 이 섹션에 정규식을 입력할 수 있습니다.

정규식을 사용하여 입력하는 패턴과 일치하는 여러 주소를 지정할 수 있습니다.</td></tr>
</table>
c. 변경 사항을 제출하고 커밋합니다.
</td></tr>
<tr><td>4단계</td><td>Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책)를 선택합니다.

a. 새 암호 해독 정책을 만듭니다.

b. 특정 애플리케이션에 대해 HTTPS 트래픽 우회를 위해 생성한 식별 프로필을 선택합니다.

c. Advanced(고급) 패널에서 URL Categories(URL 카테고리) 링크를 클릭합니다.

d. Add(추가) 열에서 을 클릭하여 3단계에서 생성한 맞춤형 URL 카테고리를 추가합니다.

e. 완료를 선택합니다.

f. Decryption Policies(해독 정책) 페이지에서 URL 필터링에 대한 링크를 클릭합니다.

g. 통과를 선택합니다.

h. 변경 사항을 제출하고 커밋합니다.

(선택 사항) 액세스 로그 정보를 보려면 %(형식 지정자)를 사용할 수 있습니다.</td></tr>
</table>

웹 요청에 대한 웹 프록시 Bypass 구성

Custom URL Categories(맞춤형 URL 카테고리)를 프록시 바이패스 목록에 추가하면 맞춤형 URL 카테고리의 모든 IP 주소 및 도메인 이름이 소스 및 목적지 모두에 대해 우회됩니다.

1단계	Web Security Manager(웹 보안 관리자) > Bypass Settings(우회 설정)를 선택합니다.
2단계	Edit Bypass Settings(우회 설정 편집)를 클릭합니다.
3단계	웹 프록시를 우회하려는 주소를 입력합니다. 참고: /0을 우회 목록의 IP에 대한 서브넷 마스크로 구성할 경우 어플라이언스는 모든 웹 트래픽을 우회합니다. 이 경우 어플라이언스는 컨피그레이션을 0.0.0.0/0으로 해석합니다.
4단계	프록시 우회 목록에 추가할 Custom URL Categories(맞춤형 URL 범주)를 선택합니다.
5단계	변경 사항을 제출하고 커밋합니다.

주의: 정규식에 대한 웹 프록시 우회를 설정할 수 없습니다.

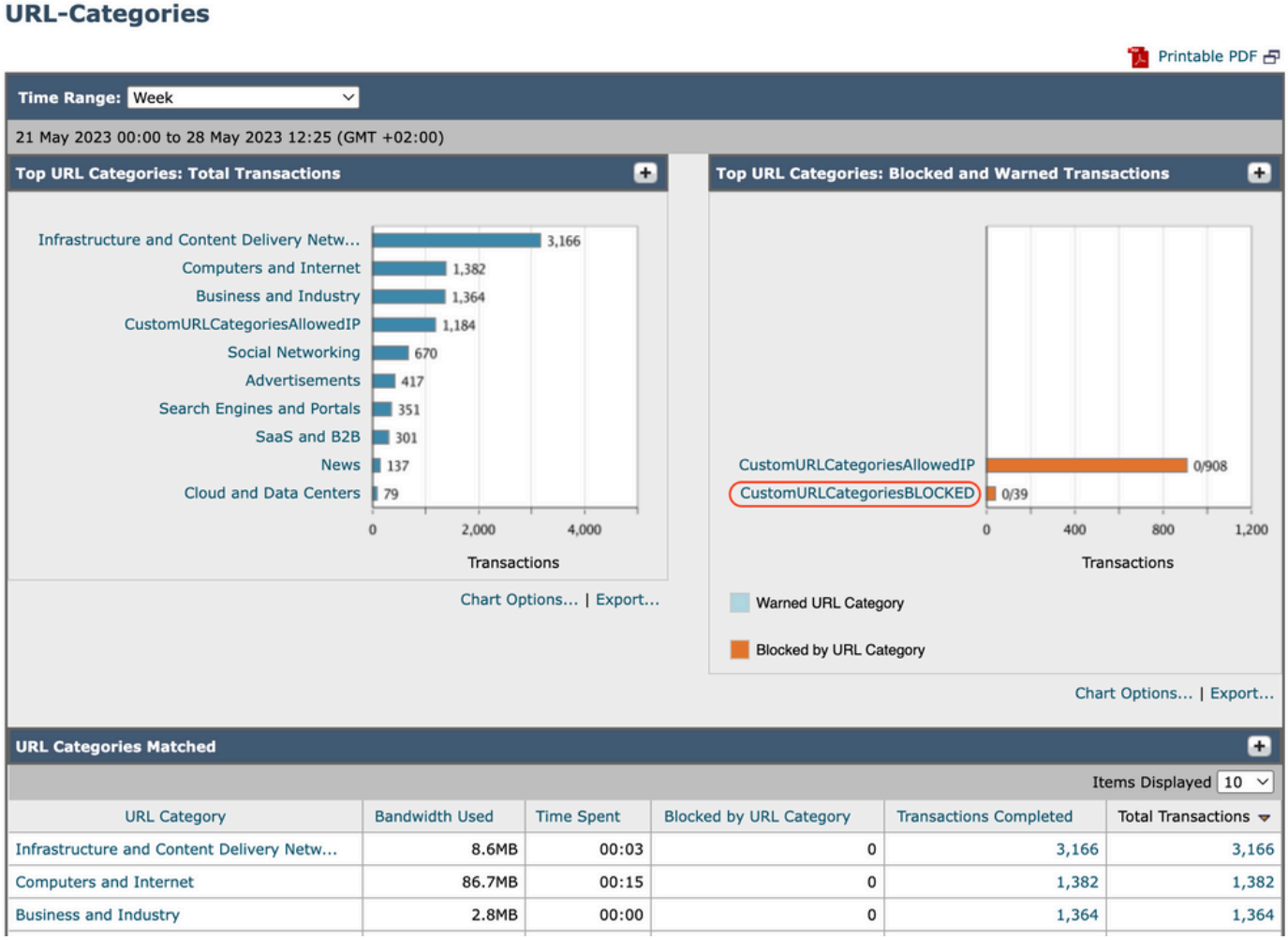
보고서

"Reporting(보고)" >> URL Categories(URL 범주) 페이지는 일치하는 상위 URL 범주 및 차단된 상위 URL 범주에 대한 정보를 포함하는 URL 통계를 종합적으로 표시합니다.

이 페이지에는 대역폭 절감 및 웹 트랜잭션에 대한 범주별 데이터가 표시됩니다.

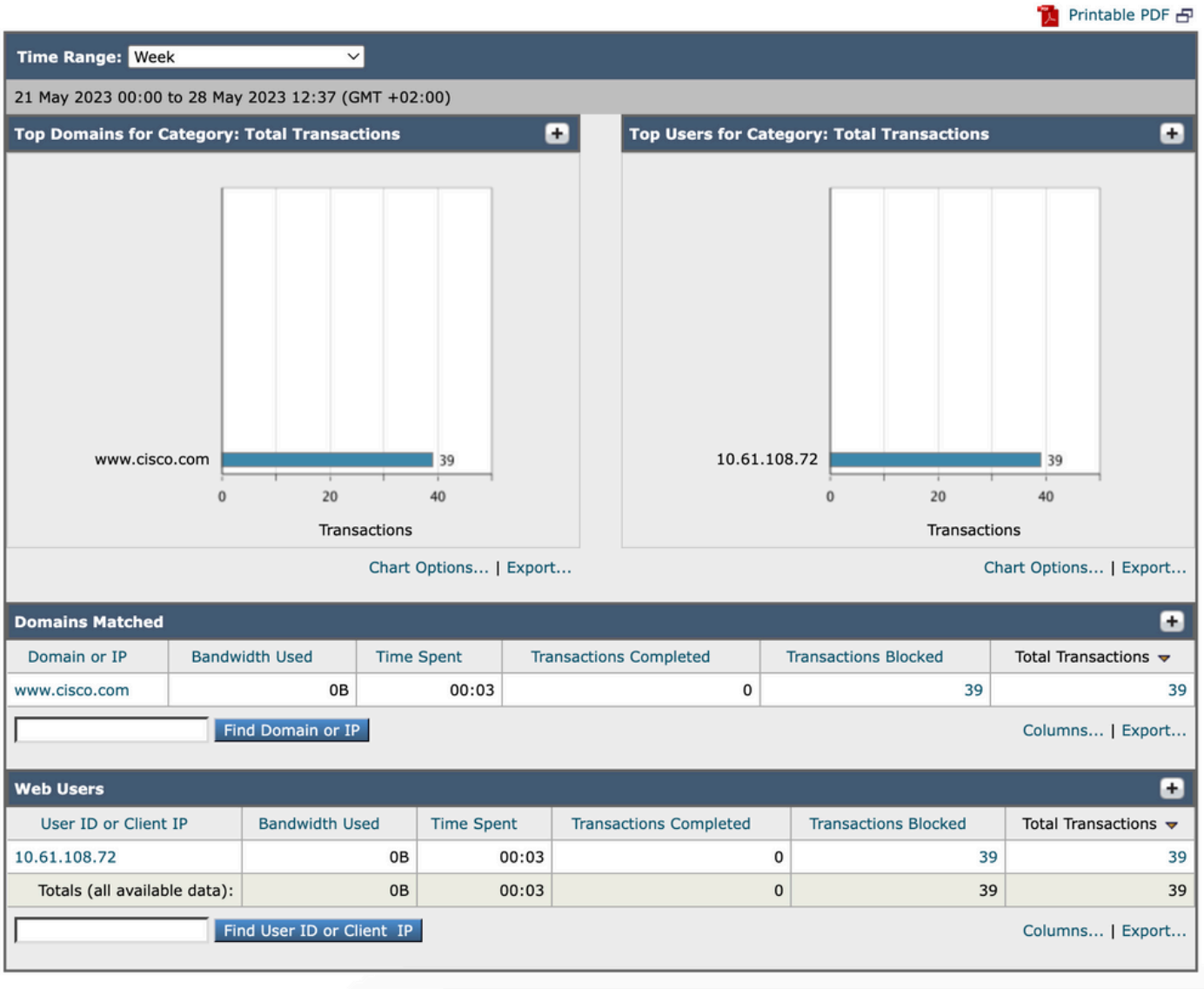
섹션	설명
시간 범위(드롭다운 목록)	보고서의 시간 범위를 선택합니다.
전체 트랜잭션별 상위 URL 범주	이 섹션에서는 사이트에서 방문하는 상위 URL 카테고리를 그래프 형식으로 나열합니다.
차단 및 경고된 트랜잭션별 상위 URL 범주	트랜잭션별로 차단 또는 경고 조치가 발생하도록 트리거한 상위 URL을 그래프 형식으로 나열합니다.

섹션	설명
일치하는 URL 범주	지정된 시간 범위 동안 URL 범주별 트랜잭션 처리와 각 범주에서 사용된 대역폭 및 소요된 시간을 표시합니다. 분류되지 않은 URL의 비율이 15-20%보다 높은 경우 다음 옵션을 고려하십시오. • 지역화된 특정 URL의 경우 맞춤형 URL 카테고리를 생성하여 특정 사용자 또는 그룹 정책에 적용할 수 있습니다. • 미분류 및 잘못 분류된 URL을 평가 및 데이터베이스 업데이트를 위해 Cisco에 보고할 수 있습니다. • Web Reputation Filter 및 Anti-Malware Filter가 활성화되었는지 확인합니다.



이미지-URL 범주 보고서

범주 이름을 클릭하면 해당 범주와 관련된 추가 세부 정보(예: 일치하는 도메인 또는 사용자 목록)를 볼 수 있습니다.



이미지 - 세부 보고서 페이지

미리 정의된 URL 범주 집합은 Web Security Appliance에서 정기적으로 자동 업데이트할 수 있습니다.

이러한 업데이트가 발생하면 이전 카테고리와 연결된 데이터가 너무 오래되어 보고서에 포함될 수 없을 때까지 이전 카테고리 이름이 보고서에 계속 표시됩니다.

URL 범주 집합 업데이트 후 생성된 보고서 데이터는 새 범주를 사용하므로, 동일한 보고서에서 이전 범주와 새 범주를 모두 볼 수 있습니다.

보고서의 URL Categories(URL 범주) 페이지에 있는 URL 통계에서는 다음 데이터를 해석하는 방법을 이해하는 것이 중요합니다.

데이터 유형	설명
우회된 URL 필터링	URL 필터링 전에 발생하는 정책, 포트 및 관리자 사용자 에이전트가 차단되었음을 나타냅니다.
분류되지 않은 URL	URL 필터링 엔진이 쿼리되었지만 일치하는 카

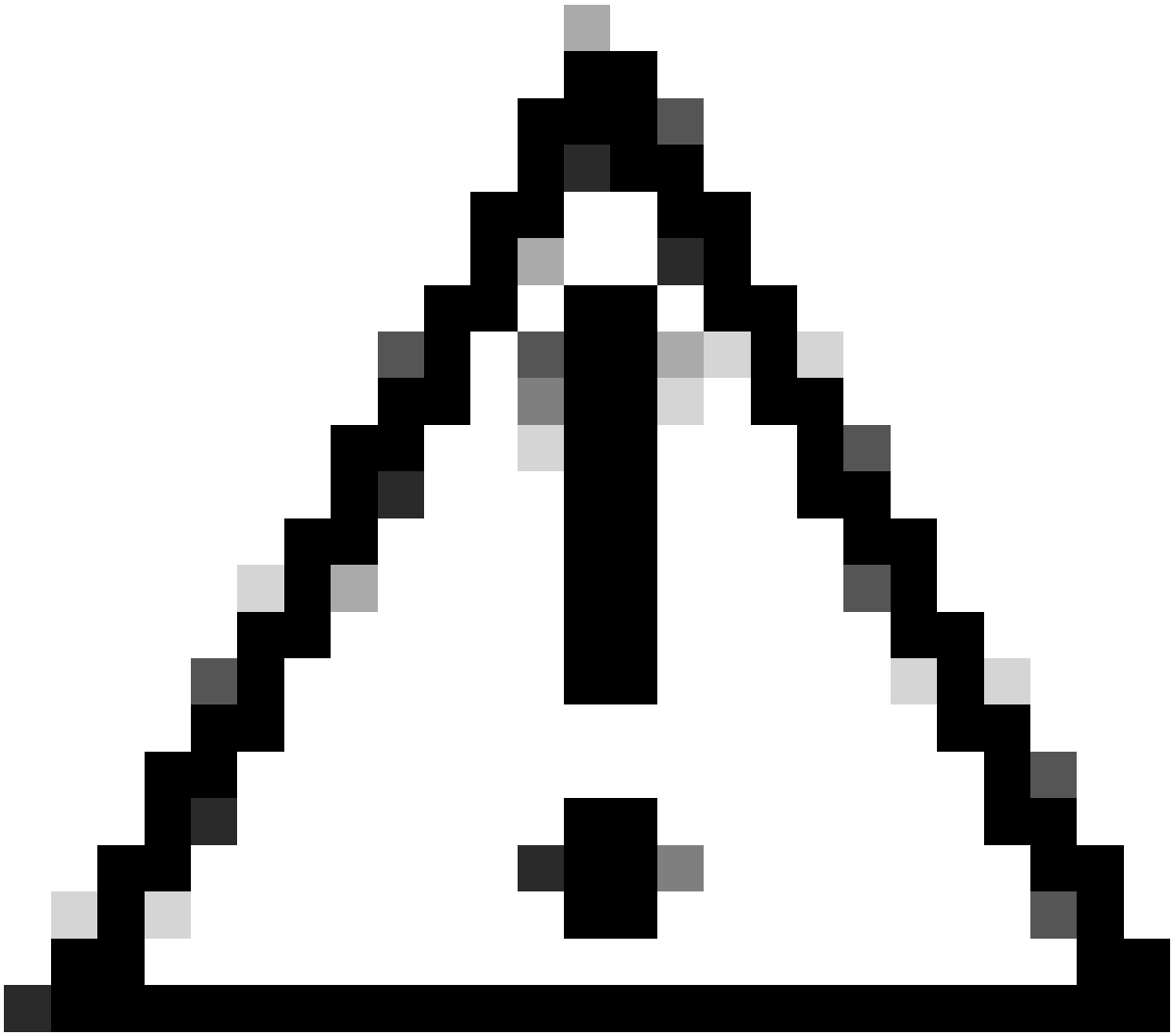
	테고리가 없는 모든 트랜잭션을 나타냅니다.

액세스 로그에서 사용자 지정 URL 범주 보기

Secure Web Appliance는 액세스 로그에서 앞에 "c_"가 오는 사용자 지정 URL 범주 이름의 처음 4자를 사용합니다.

이 예에서 범주 이름은 CustomURLCategoriesBLOCKED이고 액세스 로그에서 C_Cust를 볼 수 있습니다.

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



주의: Sawmill을 사용하여 액세스 로그를 구문 분석하는 경우 맞춤형 URL 범주 이름을 고려하십시오. 사용자 지정 URL 카테고리의 처음 4개 문자에 공백이 포함된 경우 Sawmill은 액세스 로그 항목을 제대로 구문 분석할 수 없습니다. 대신 처음 4개 문자에 지원되는 문자

만 사용하십시오.

팁: 액세스 로그에 사용자 지정 URL 범주의 전체 이름을 포함하려면 %XF 형식 지정자를 액세스 로그에 추가하십시오.

웹 액세스 정책 그룹에 Monitor(모니터링)로 설정된 맞춤형 URL 카테고리가 있고 다른 구성 요소(예: Web Reputation Filters 또는 Different Verdict Scanning(DVS) 엔진)가 맞춤형 URL 카테고리의 URL에 대한 요청을 허용하거나 차단하도록 최종 결정하는 경우 요청에 대한 액세스 로그 항목에 맞춤형 URL 카테고리 대신 사전 정의된 URL 카테고리가 표시됩니다.

액세스 로그에서 사용자 지정 필드를 구성하는 방법에 대한 자세한 내용은 Configure Performance Parameter in Access Logs - Cisco를 참조하십시오.

문제 해결

범주가 일치하지 않음

선택이 예상대로 되지 않은 경우 액세스 로그에서 해당 요청이 어떤 Custom URL Category에 속하는지 확인할 수 있습니다.

- 요청이 다른 사용자 지정 URL 범주로 분류된 경우 중복 URL 또는 다른 범주의 일치하는 정규식을 확인하거나 사용자 지정 URL 범주를 맨 위로 이동하고 다시 테스트합니다. 일치하는 사용자 지정 URL 범주를 신중하게 검사하는 것이 좋습니다.

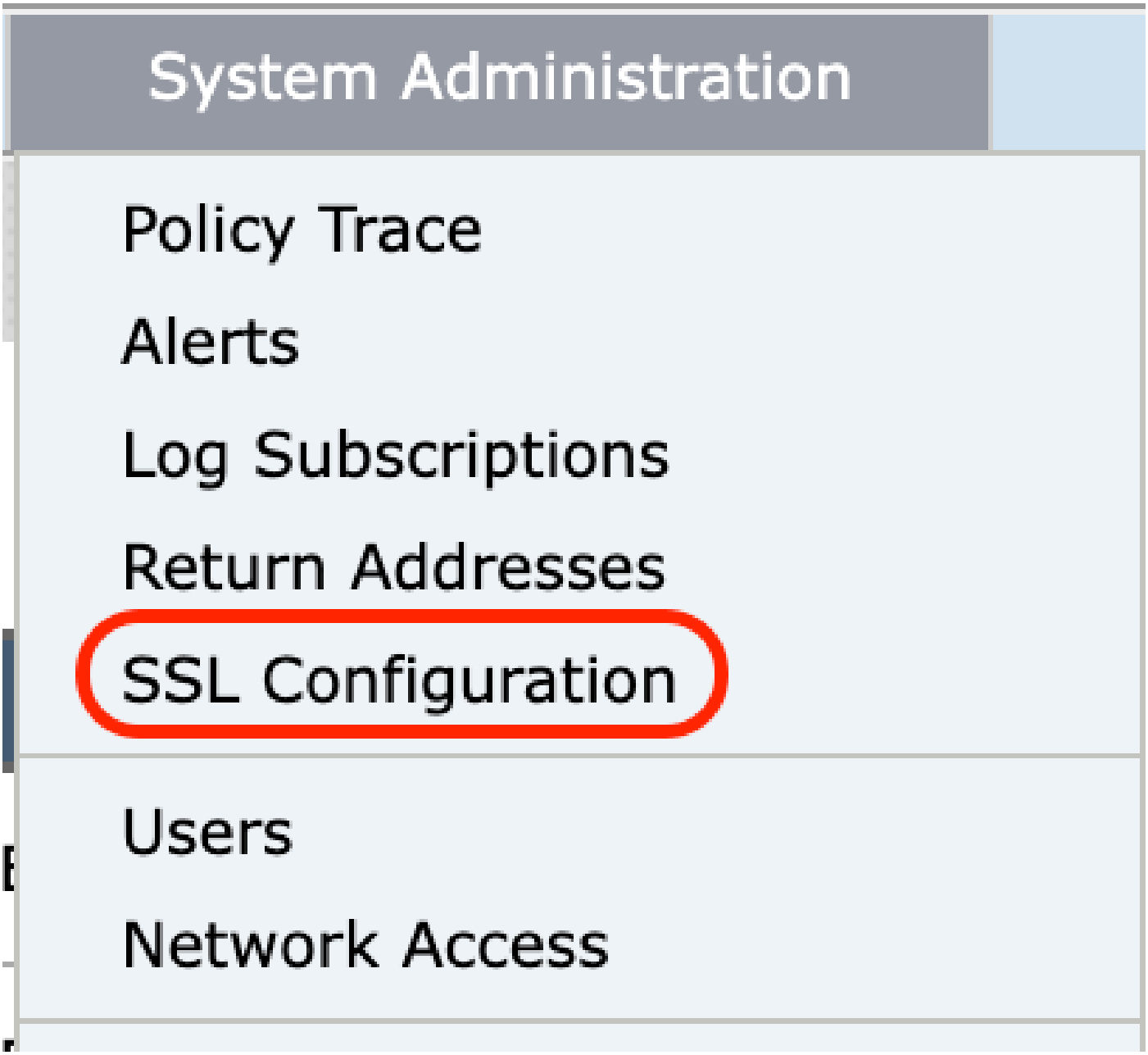
- 요청이 미리 정의된 범주로 분류된 경우 기존 맞춤형 URL 범주의 조건을 확인합니다. 일치하는 경우 IP 주소를 추가하고 테스트하거나 오타 및 올바른 정규식이 사용되는지 확인합니다(있는 경우).

미리 정의된 범주가 최신 상태가 아님

미리 정의된 범주가 최신 상태가 아니거나 액세스 로그에 URL 범주 섹션에 "err"이 표시되는 경우 업데이터에 대해 TLSv1.2가 활성화되어 있는지 확인합니다.

업데이터 SSL 컨피그레이션을 변경하려면 GUI에서 다음 단계를 수행합니다.

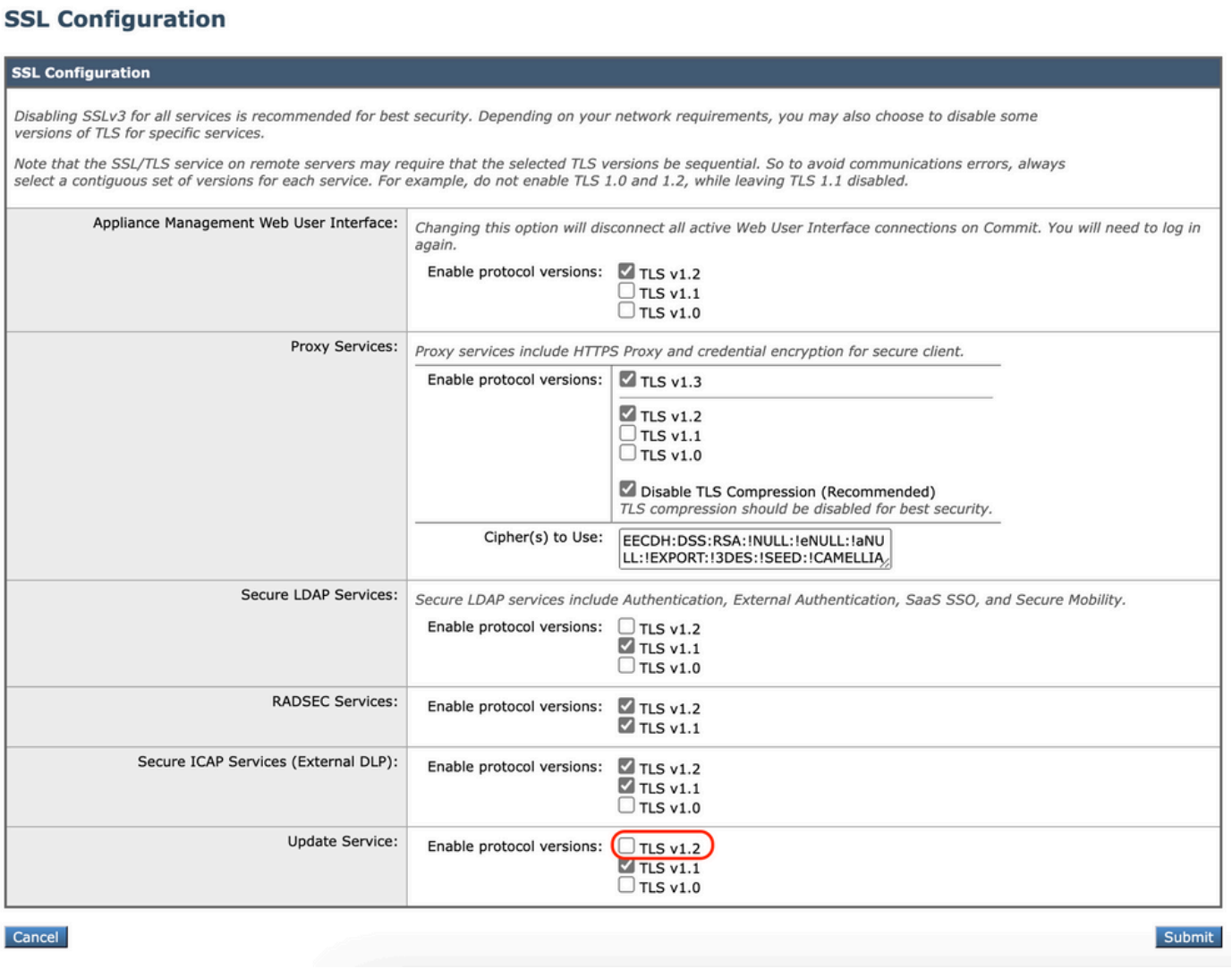
1단계. System Administration(시스템 관리)에서 SSL Configuration(SSL 컨피그레이션)을 선택합니다



이미지 - ssl 컨피그레이션

2단계. Edit Settings(설정 편집)를 선택합니다.

3단계. 서비스 업데이트 섹션에서 TLSv1.2를 선택합니다



이미지 - 업데이트 서비스 TLSv1.2

4단계. 변경 내용을 제출하고 커밋합니다

업데이터 SSL 컨피그레이션을 변경하려면 CLI에서 다음 단계를 수행합니다.

1단계. CLI에서 sslconfig를 실행합니다

2단계. version을 입력하고 Enter 키를 누릅니다

3단계. 업데이터 선택

4단계. TLSv1.2를 선택합니다

5단계. Enter를 눌러 마법사를 종료합니다

6단계. 변경 사항을 커밋합니다.

```
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 sequentia
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, Secu
        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.
```

참조

Cisco Web Security Appliance 모범 사례 지침 - Cisco

BRKSEC-3303(ciscolive)

AsyncOS 14.5 for Cisco Secure Web Appliance - GD(General Deployment) - 연결, 설치 및 구성
[Cisco Secure Web Appliance] 사용 설명서 - Cisco

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.