Secure Web Appliance에서 Google AI 모드 차단

목차

소개

이 문서에서는 Secure Web Appliance가 Google AI 모드에 대한 HTTPS 요청을 차단하도록 구성되도록 수행하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리
- 기본 네트워킹 및 프록시 프로토콜
- SWA의 암호 해독 프로세스
- 정규식

Cisco에서는 다음과 같은 툴을 설치하는 것이 좋습니다.

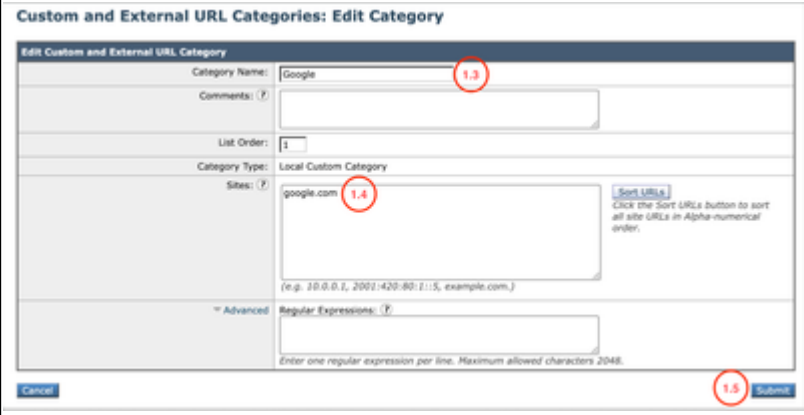
- 물리적 또는 가상 SWA
- SWA 그래픽 사용자 인터페이스(GUI)에 대한 관리 액세스

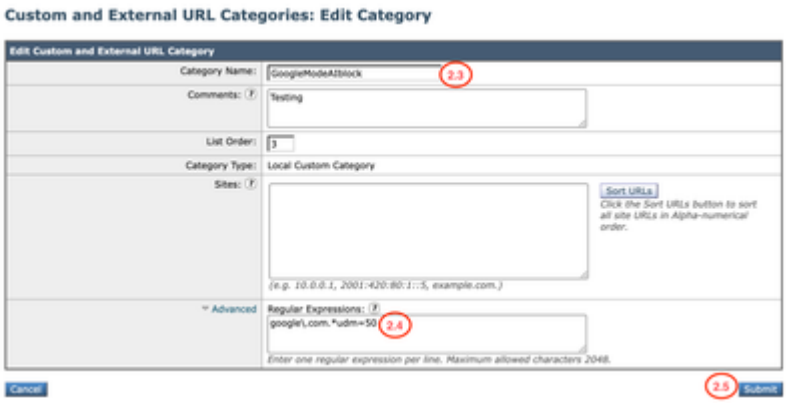
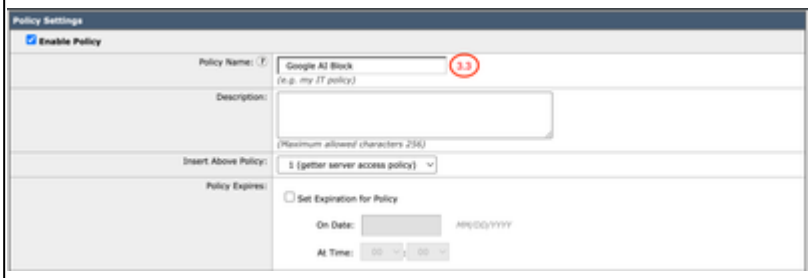
사용되는 구성 요소

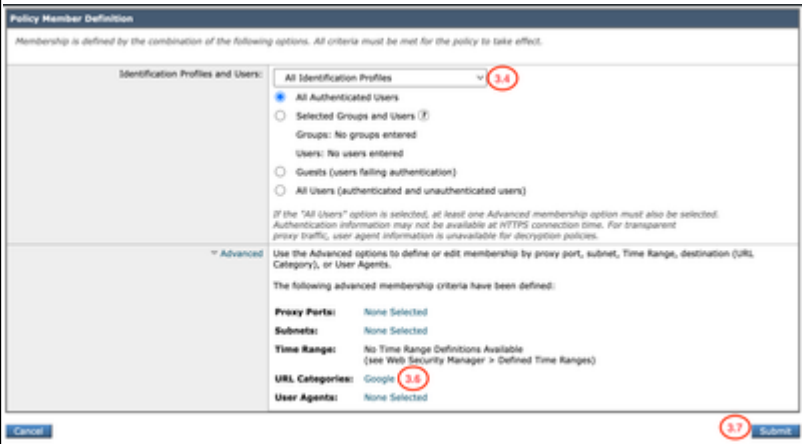
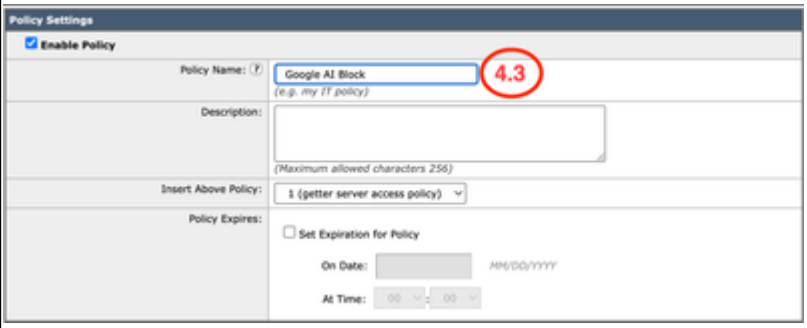
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

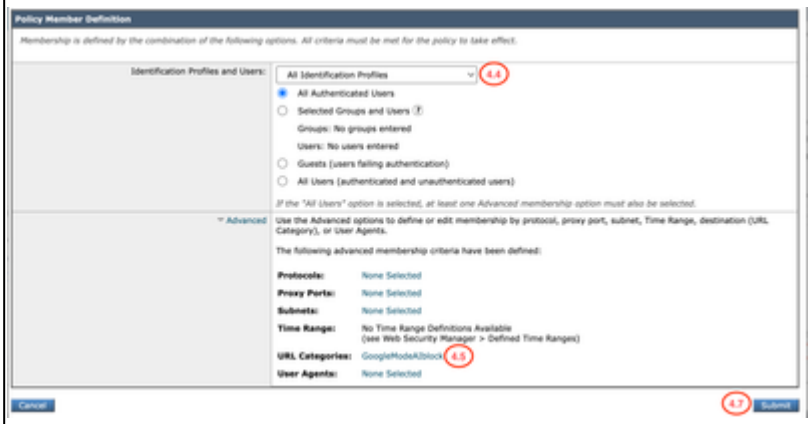
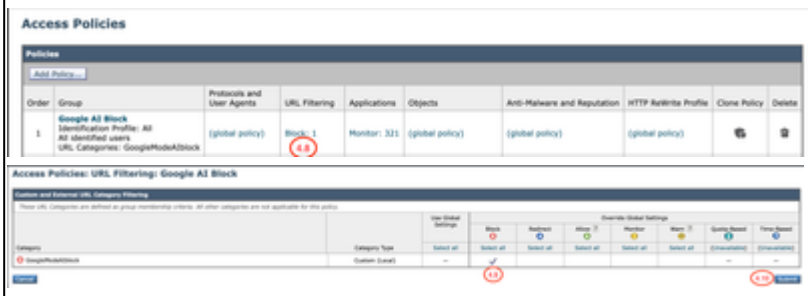
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성 단계

1단계. Google 웹 사이트에 대한 맞춤형 URL 카테고리를 생성합니다.	1.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하여 Custom(사용자 지정) 및 External URL Categories(외부 URL 범주)를 선택합니다. 1.2단계. Add Category(카테고리 추가)를 클릭하여 새 맞춤형 URL 카테고리를 생성합니다. 1.3단계. 새 범주의 이름을 입력합니다. 1.4단계. Sites(사이트) 섹션에서 이 URL을 정의합니다. `google.com` 1.5단계. 변경 사항을 제출합니다. 
2단계.Google AI 모드에 대한 사용자 지정 URL 카테고리를 생성합니다.	2.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하여 Custom(사용자 지정) 및 External URL Categories(외부 URL 범주)를 선택합니다. 2.2단계. Add Category(카테고리 추가)를 클릭하여 새 맞춤형 URL 카테고리를 생성합니다. 2.3단계. 신규 범주의 이름을 입력합니다.

	2.4단계. Regular Expressions 섹션에서 이 URL을 정의합니다. `google\.com.*udm=50` 2.5단계. 변경 사항을 제출합니다. 팁: 맞춤형 URL 카테고리 구성 방법에 대한 자세한 내용은 Configure Custom URL Categories in Secure Web Appliance - Cisco를 참조하십시오. 
3단계. Google의 트래픽을 해독합니다.	3.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다 3.2단계. Add Policy(정책 추가)를 클릭합니다. 3.3단계. 새 정책의 이름을 입력합니다.  3.4단계. (선택 사항) 이 정책을 적용해야 하는 식별 프로필을 선택합니다. 3.5단계. Policy Member Definition(정책 구성원 정의) 섹션에서 URL Categories(URL 범주) 링크를 클릭하여 Custom URL Category(맞춤형 URL 범주)를 추가합니다.

	3.6단계. 1단계에서 생성한 URL 범주를 선택합니다. 3.7단계. Submit(제출)을 클릭합니다.  3.8단계. Decryption Policies(암호 해독 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다. 3.9단계. Custom URL Category(맞춤형 URL 카테고리)에 대한 작업으로 Decrypt(해독)를 선택합니다. 3.10단계. 제출을 클릭합니다. 
4단계. Google AI 모드 트래픽을 차단합니다.	4.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 Access Policies(액세스 정책)를 선택합니다. 4.2단계. Add Policy(정책 추가)를 클릭합니다. 4.3단계. 새 정책의 이름을 입력합니다.  4.4단계. (선택 사항) 이 정책을 적용해야 하는 식별 프로필을 선택합니다.

	4.5단계. Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리) 링크를 클릭하여 Custom URL Category(맞춤형 URL 카테고리)를 추가합니다. 4.6단계. 2단계에서 생성한 URL 범주를 선택합니다. 4.7단계. Submit(제출)을 클릭합니다.  4.8단계. Access Policies(액세스 정책) 페이지에서 URL Filtering(URL 필터링)에서 링크를 클릭하여 새 정책을 구성합니다. 4.9단계. Custom URL Category(맞춤형 URL 카테고리)에 대한 작업으로 Block(차단)을 선택합니다. 4.10단계. 제출을 클릭합니다.  4.11단계. 변경 사항을 커밋합니다.

다음을 확인합니다.

컨피그레이션 설정이 완료되면 Google AI Block에 대해 생성한 Custom Category(맞춤형 카테고리)에서 탐지되는 대로 Google AI 트래픽이 액세스 로그에서 Block(차단)으로 처리됩니다.

<#root>

```
1779219170.427 101 10.184.103.26
```

TCP_DENIED_SSL/403

```
 0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo
```

BLOCK_CUSTOMCAT_12-Google_AI_Block

```
-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"
```

구글 AI 모드를 통한 검색질의 요청이 차단되어 이 최종 사용자 알림이 표시된다.

다른 모든 Google 트래픽은 계속 허용됩니다.

관련 정보

WSA에서 맞춤형 URL 범주 정의

AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서

Secure Web Appliance에서 암호 해독 인증서 구성

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.