Secure Web Appliance에서 업로드 트래픽 차단

목차

소개

이 문서에서는 SWA(Secure Web Appliance)의 특정 웹 사이트에 대한 업로드 트래픽을 차단하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 그래픽 사용자 인터페이스(GUI)에 액세스
- SWA에 대한 관리 액세스.

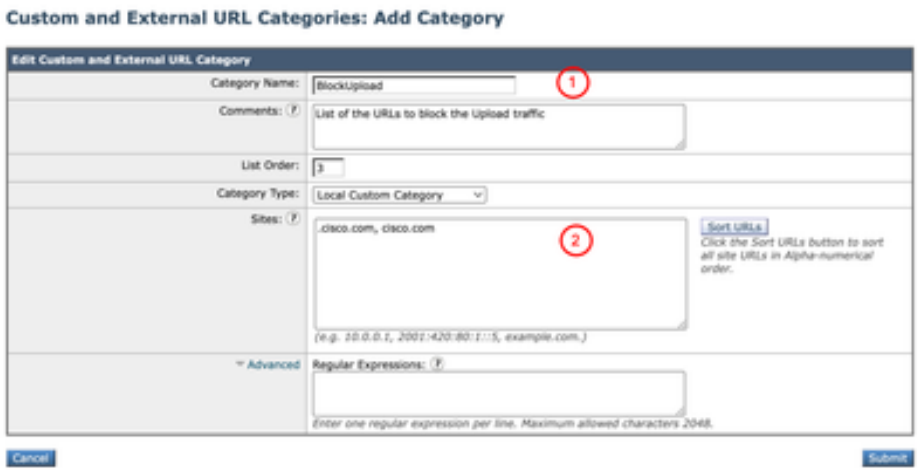
사용되는 구성 요소

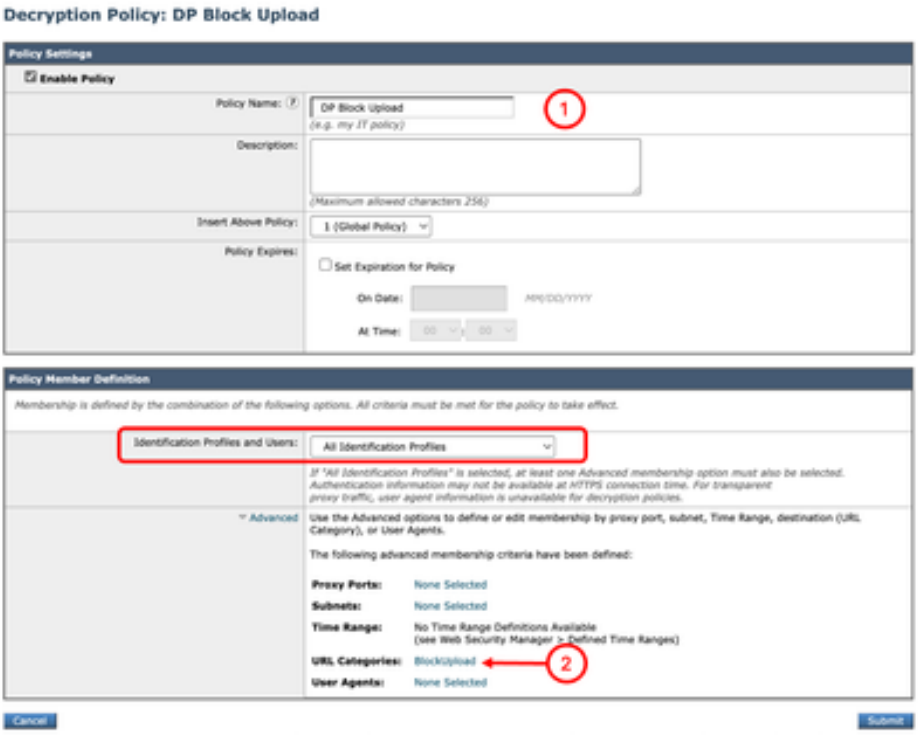
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

컨피그레이션 단계

1단계. 웹 사이트에 대한 맞춤형 URL 카테고리를 생성합니다.	1.1단계. GUI에서 Web Security Manager(Web Security Manager)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. 업로드 트래픽을 차단하려는 웹 사이트의 도메인 및/또는 하위 도메인을 정의합니다(이 예에서는 cisco.com 및 모든 하위 도메인). 1.5단계. 변경 사항을 제출합니다.  이미지 - 사용자 지정 URL 범주 만들기 팁: 맞춤형 URL 카테고리를 구성하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html을 참조하십시오.
2단계. URL의 트래픽 해독	2.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다 2.2단계. Add Policy(정책 추가)를 클릭합니다. 2.3단계. 새 정책의 Name을 입력합니다. 2.4단계. (선택 사항) 이 정책을 적용할 식별 프로필을 선택합니다. 2.5단계. Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리) 링크를 클릭하여 Custom URL Category(맞춤형 URL 카테고리)를 추가합니다. 2.6단계.1단계에서 생성한 URL 카테고리를 선택합니다. 2.7단계. Submit(제출)을 클릭합니다.

<table>
<tr>
<td></td>
<td>


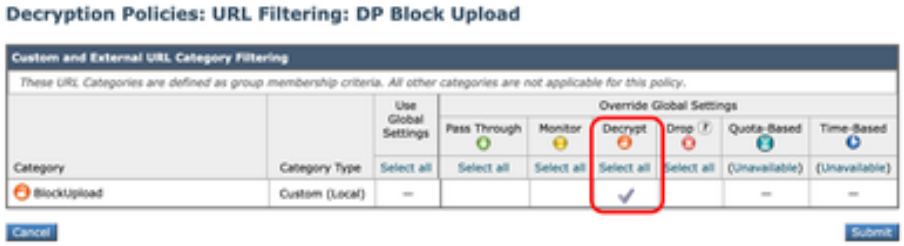
이미지 - 암호 해독 정책 생성

2.8단계. Decryption Policies(암호 해독 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.

이미지 - URL 필터링 선택

2.9단계. Custom URL Category(맞춤형 URL 카테고리)에 대한 작업으로 Decrypt(해독)를 선택합니다.

2.10단계. Submit(제출)을 클릭합니다.



Image(이미지) - Set Decrypt as Action(해독을 작업으로 설정)</td>
</tr>
<tr>
<td>3단계. 업로드 트래픽 차단</td>
<td>3.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하여 Cisco Data Security를 선택합니다.</td>
</tr>
</table>

3.2단계. Add Policy(정책 추가)를 클릭합니다.

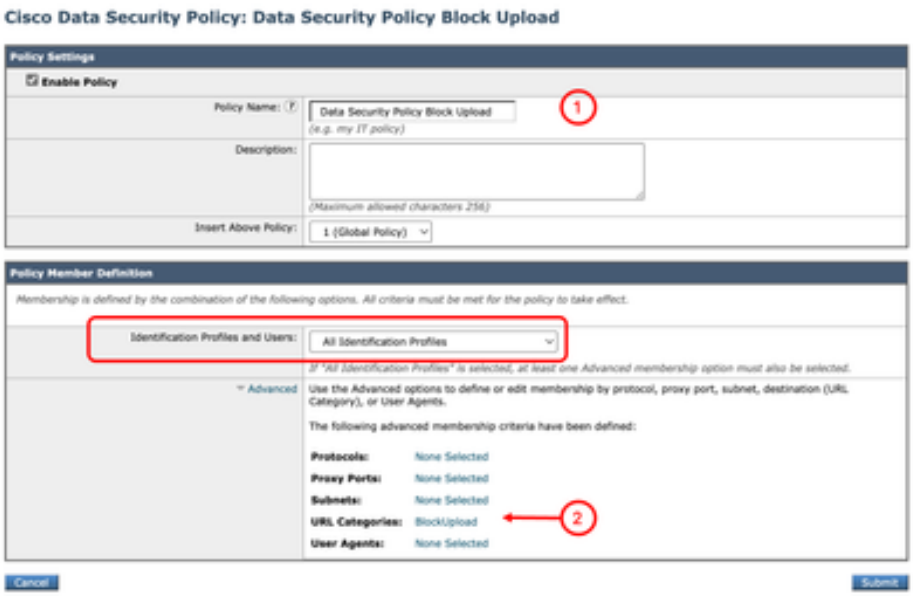
3.3단계. 새 정책의 Name을 입력합니다.

3.4단계. (선택 사항) 이 정책을 적용할 식별 프로필을 선택합니다.

3.5단계. Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리) 링크를 클릭하여 Custom URL Category(맞춤형 URL 카테고리)를 추가합니다.

3.6단계.1단계에서 생성한 URL 카테고리를 선택합니다.

3.7단계. Submit(제출)을 클릭합니다.



이미지 - Cisco 데이터 보안 정책

팁: 보고를 위해 다른 액세스/암호 해독 정책과 동일하지 않은 이름을 선택하는 것이 가장 좋습니다.

3.8단계. Cisco Date Security Policy(Cisco 날짜 보안 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.

이미지 - URL 필터링 선택

3.9단계. Custom URL Category(맞춤형 URL 카테고리)에 대한 작

	업으로 Block(차단)을 선택합니다. 3.10단계. Submit(제출)을 클릭합니다.  이미지 - 업로드 차단 3.11단계. 변경 사항을 커밋합니다.

보고 및 로그

로그

데이터 보안 로그의 기본 로깅 이름인 idsdatalos_logs를 선택하여 CLI에서 업로드 트래픽과 관련된 로그를 볼 수 있습니다.

다음 단계를 사용하여 로그에 액세스합니다.

1단계. CLI에 로그인합니다

2단계. grep를 입력하고 Enter 키를 누릅니다.

3단계. idsdatalos_logs와 연결된 번호를 찾아 입력합니다.

- 유형: "데이터 보안 로그"
- 검색: FTP Poll(FTP 폴링)을 클릭하고 Enter 키를 누릅니다.

4단계(선택 사항) 키워드를 기준으로 팬 필터링하도록 정규식을 입력하거나 Enter를 눌러 모든 로그를 볼 수 있습니다

5단계. (선택 사항) 이 검색에서 대/소문자를 구분하지 않으시겠습니까? [Y]> 4단계에서 키워드를 선택한 경우 대/소문자를 구분하지 않고 필터를 선택할 수 있습니다.

6단계(선택 사항) 일치하지 않는 라인을 검색하시겠습니까? [N]>4단계에서 정의한 선택한 키워드를 제외한 모든 로그를 필터링해야 하는 경우 이 섹션을 사용할 수 있습니다. 그렇지 않으면 Enter 키를 누를 수 있습니다.

7단계(선택 사항) 로그를 테일링하시겠습니까? [N]> 라이브 로그를 확인해야 하는 경우 Y를 입력하고 Enter 키를 누릅니다. 그렇지 않으면 Enter를 눌러 사용 가능한 모든 로그를 표시합니다.

8단계(선택 사항) 출력을 페이지 매김하시겠습니까? [N]> 페이지당 결과를 확인해야 하는 경우 Y를 입력하고 Enter를 누르거나 Enter를 눌러 기본값 [N]을 사용합니다.

보고

Cisco Data Security 정책 이름으로 차단된 업로드 트래픽의 보고서를 보려면 Web Tracking(웹 추적) 보고서를 생성할 수 있습니다.

다음 단계를 사용하여 보고서를 생성합니다.

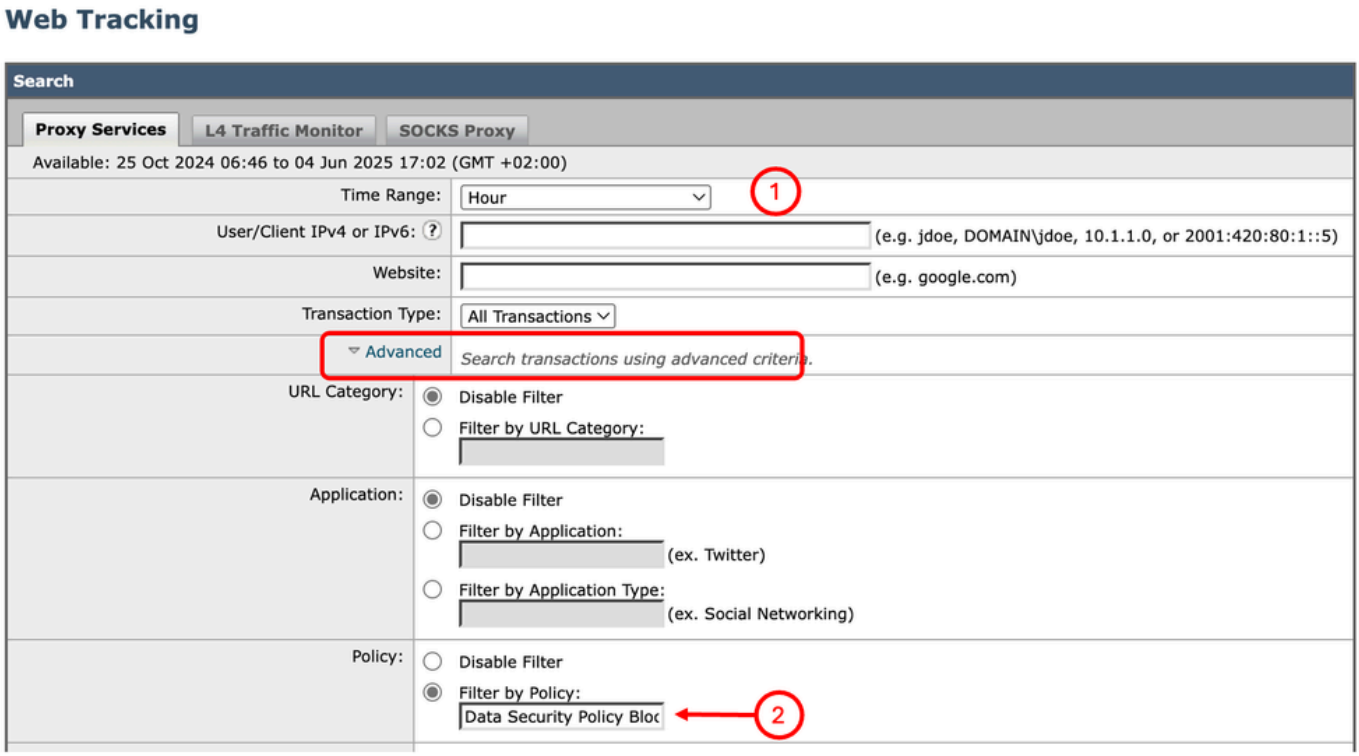
1단계. GUI에서 Reporting(보고)을 선택하고 Web Tracking(웹 추적)을 선택합니다.

2단계. 원하는 시간 범위를 선택합니다.

3단계. 고급 링크를 눌러 고급 기준을 사용하여 트랜잭션을 검색합니다.

4단계. Policy(정책) 섹션에서 Filter by Policy(정책으로 필터링)를 선택하고 이전에 생성한 Cisco Data Security의 이름을 입력합니다.

5단계. 검색을 눌러 보고서를 검토합니다.



이미지 - 웹 추적 보고서 필터링

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Cisco Secure Email and Web Virtual Appliance 설치 설명서
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
- Secure Web Appliance 모범 사례 사용
- Secure Web Appliance용 방화벽 구성

- Secure Web Appliance에서 암호 해독 인증서 구성
- SWA에서 SNMP 구성 및 문제 해결
- Microsoft Server를 사용하여 Secure Web Appliance에서 SCP 푸시 로그 구성
- SWA에서 특정 YouTube 채널/비디오 활성화 및 나머지 YouTube 차단
- Secure Web Appliance의 HTTPS 액세스 로그 형식 이해
- Secure Web Appliance 로그 액세스
- Secure Web Appliance에서 인증 우회
- Secure Web Appliance에서 트래픽 차단
- Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회

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.