게스트 액세스를 허용하도록 Secure Web Appliance 구성

목차

소개

이 문서에서는 암호 해독 인증서를 설치하지 않은 사용자가 SWA(Secure Web Appliance)를 통해 인터넷에 액세스할 수 있도록 허용하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- 라이센스가 활성화되었거나 설치되었습니다.
- 설치 마법사가 완료되었습니다.

- SWA GUI(Graphical User Interface)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.

시나리오 개요

이 문서에서는 10.10.10.0/24 Wi-Fi 서브넷 내의 네트워크 액세스 제어 시나리오에 대해 설명합니다. 환경은 각기 다른 보안 및 액세스 정책을 필요로 하는 두 개의 고유한 사용자 그룹으로 구성됩니다.

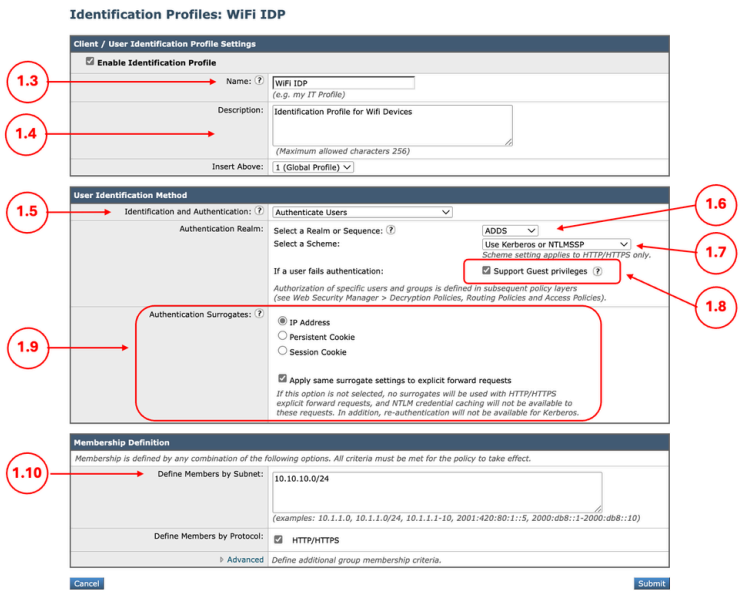
- 관리되는 디바이스: 회사에서 지급한 랩톱으로, 완전히 인증되었으며 SWA 암호 해독 인증서가 설치되어 있습니다. 이러한 디바이스는 신뢰할 수 있으며 일반적으로 표준 기업 액세스 정책의 적용을 받습니다.
- 관리되지 않는/게스트 디바이스: 인증되지 않았고 SWA 암호 해독 인증서가 없는 개인 랩톱 및 모바일 장치.

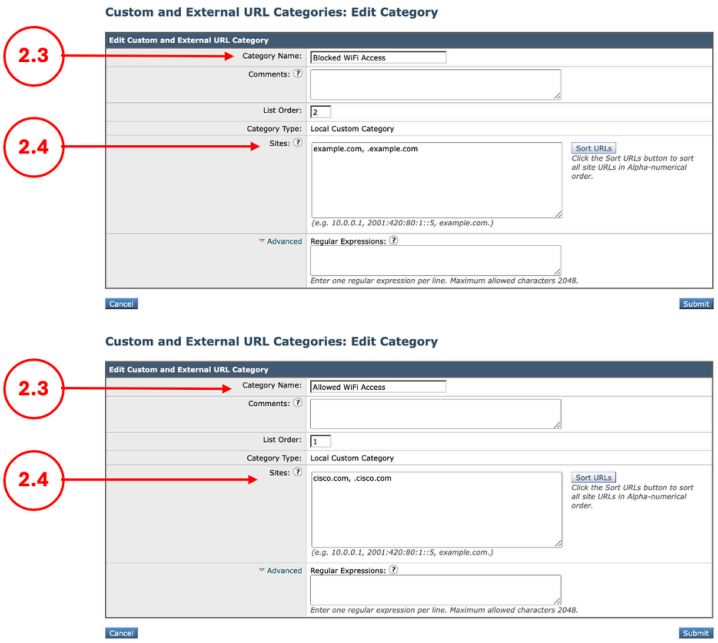
목표:
이 회사는 관리되지 않는 장치에 대한 제한적인 웹 액세스 정책을 구현하여, 회사 리소스가 안전하게 유지되도록 하면서 허용된 URL의 특정 하위 집합으로 연결을 제한하는 것을 목표로 합니다.

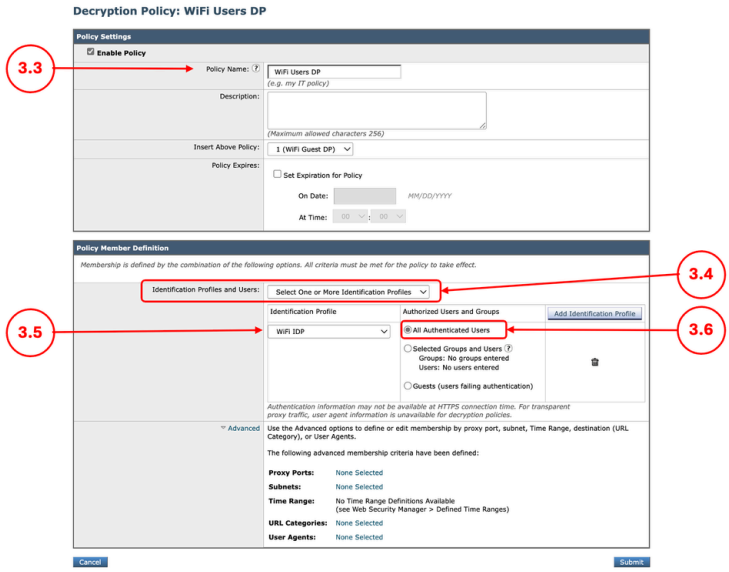
참고: Decryption Certificate는 관리되지 않는 디바이스에서 신뢰되지 않으므로 HTTPS 트래픽의 암호를 해독할 수 없으며 작업을 통과하도록 설정해야 합니다.

컨피그레이션 단계

1단계. 식별 프로필을 생성합니다.	1.1단계. SWA GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 Identification Profile(식별 프로필)을 선택합니다. 1.2단계. Add Identification Profile(식별 프로필 추가)을 클릭합니다. 1.3단계. 프로파일의 이름을 정의합니다. 단계 1.4. (선택사항) 설명을 정의합니다. 1.5단계. Authenticate Users in Identification and Authentication(식별 및 인증에서 사용자 인증)을 선택합니다. 1.6단계. Select a Realm or Sequence(영역 또는 시퀀스 선택)에서 Active Directory 영역을 선택합니다. 1.7단계. Select a Scheme(체계 선택)에서 원하는 인증 프로토콜을 선택합니다.

	팁: 체계 선택 목록에서 기본 인증을 선택하지 마십시오. 1.8단계. Support Guest privileges(게스트 권한 지원) 확인란을 선택합니다. 1.9단계(선택 사항) 설계에 따라 Apply same surrogate settings to explicit forward requests를 활성화하여 Surrogate를 활성화할 수 있습니다. 주의: 트래픽을 해독할 수 없으므로 투명한 배포에서 Persistent Cookie 또는 Session Cookie를 선택하지 않습니다. 1.10단계. IP 주소 서브넷을 정의하고 서브넷별 구성원 정의를 참조하십시오. 1.11단계. 변경 사항을 제출 및 커밋합니다.  이미지 - 식별 프로필 정의
2단계. (선택 사항) 허용 및 차단된 URL에 대한 맞춤형 URL 카테고리를 생성합니다	2.1단계.GUI에서 Web Security Manager로 이동하고 Custom and External URL Categories(사용자 지정 및 외부 URL 범주)를 선택합니다. 2.2단계.Add Category(카테고리 추가)를 클릭하여 새 맞춤형 URL 카테고리를 생성합니다. 2.3단계.새 범주의 이름을 입력합니다. 2.4단계.액세스를 차단할 웹 사이트의 도메인 및/또는

	하위 도메인을 정의합니다. 2.5단계.변경 내용을 제출합니다. 2.6단계. 액세스를 허용하는 웹 사이트에 대해 URL 카테고리를 생성하려면 동일한 단계를 사용합니다.  이미지 - 사용자 지정 URL 범주 정의
3단계. 관리되는 디바이스에 대한 암호 해독 정책 생성	3.1단계. GUI에서 Web Security Manager로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다 3.2단계. Add Policy(정책 추가)를 클릭합니다. 3.3단계. 새 정책의 EnterName을 입력합니다. 3.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다. 3.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다. 3.6단계. All Authenticated Users(인증된 모든 사용자)를 선택합니다. 3.7단계.Submit(제출)을 클릭합니다.



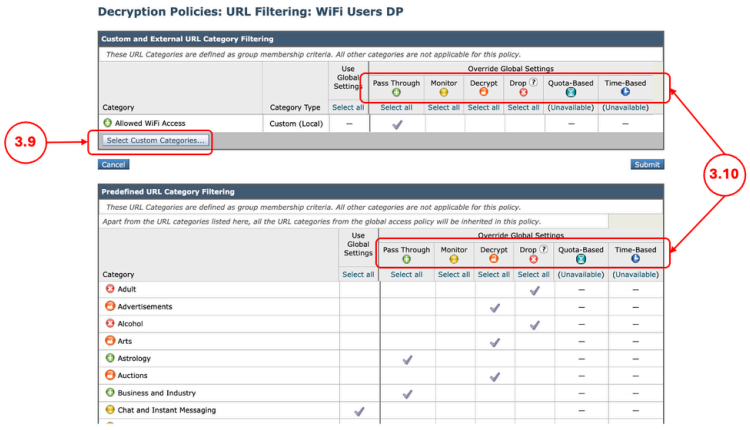
관리되는 디바이스에 대한 암호 해독 정책 생성

3.8단계. Decryption Policies(암호 해독 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.

3.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다

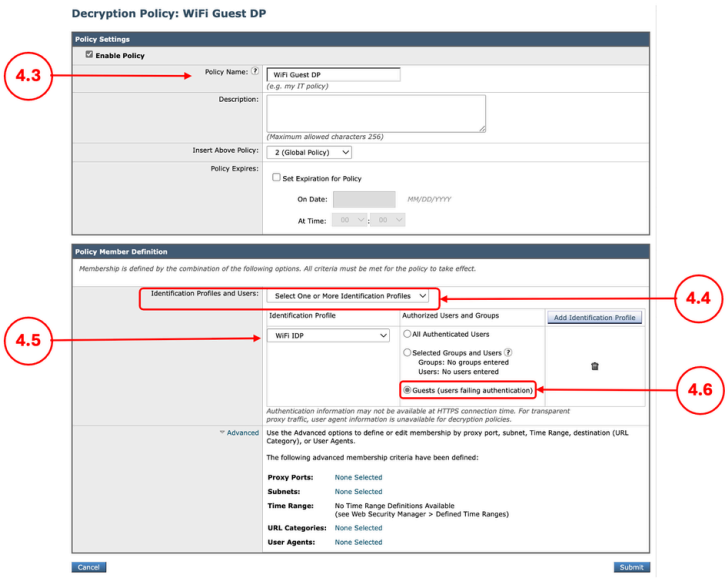
3.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링 및 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다.

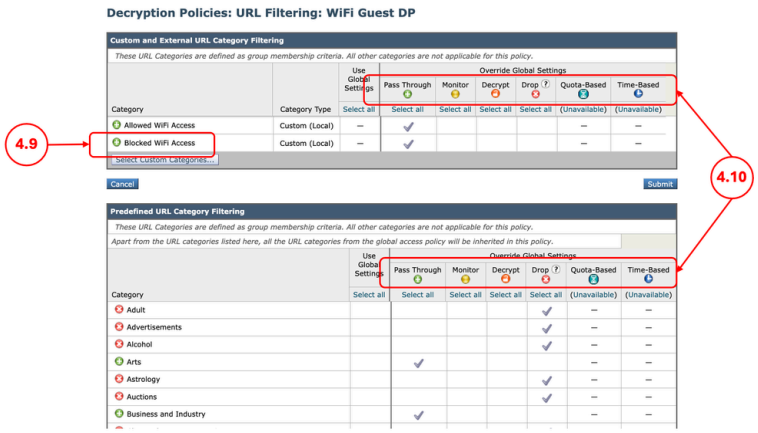
3.11단계. Submit(제출)을 클릭합니다.



이미지 - 암호 해독 정책에 대한 작업 구성

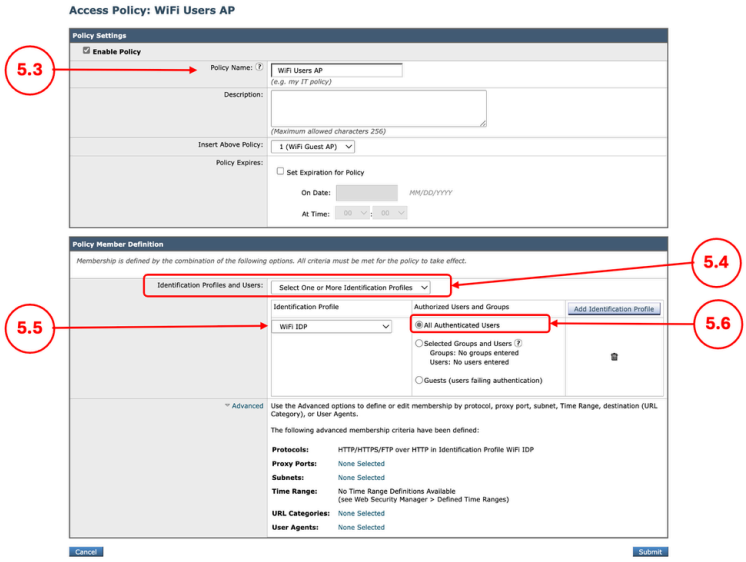
4단계. 관리되지 않는 장치에 대한 암	4.1단계. GUI에서 Web Security Manager로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다

호 해독 정책 만들기	4.2단계. Add Policy(정책 추가)를 클릭합니다. 4.3단계. 새 정책의 EnterName을 입력합니다. 4.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다. 4.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다. 4.6단계. Guests(사용자 인증 실패)를 선택합니다. 4.7단계.Submit(제출)을 클릭합니다.  관리되지 않는 장치에 대한 암호 해독 정책 만들기 4.8단계. Decryption Policies(암호 해독 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다. 4.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다 4.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링 및 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다. 참고: SWA 해독 인증서가 관리되지 않는 디바이스에서 신뢰되지 않으므로 Decrypt를 작업으로

	사용하지 마십시오.  이미지 - 관리되지 않는 디바이스에 대한 암호 해독 작업 4.11단계 Uncategorized URLs(분류되지 않은 URL) 섹션에서 아래로 스크롤하여 적절한 작업을 선택합니다.  이미지 - 분류되지 않은 URL 팁: 보안 관점에서는 URL에 액세스가 필요한 경우 Drop(삭제)으로 설정하는 것이 가장 좋습니다. 정책에 할당된 Custom URL Category(맞춤형 URL 카테고리)에서 작업을 추가할 수 있습니다. 4.12단계. Submit(제출)을 클릭합니다.
5단계. 관리되는 디바이스에 대한 액세스 정책 생성	5.1단계. GUI에서 Web Security Manager로 이동하고 Access Policies(액세스 정책)를 선택합니다 5.2단계. Add Policy(정책 추가)를 클릭합니다. 5.3단계. 새 정책의 EnterName을 입력합니다. 5.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다. 5.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다.

5.6단계. All Authenticated Users(인증된 모든 사용자)를 선택합니다.

5.7단계.Submit(제출)을 클릭합니다.

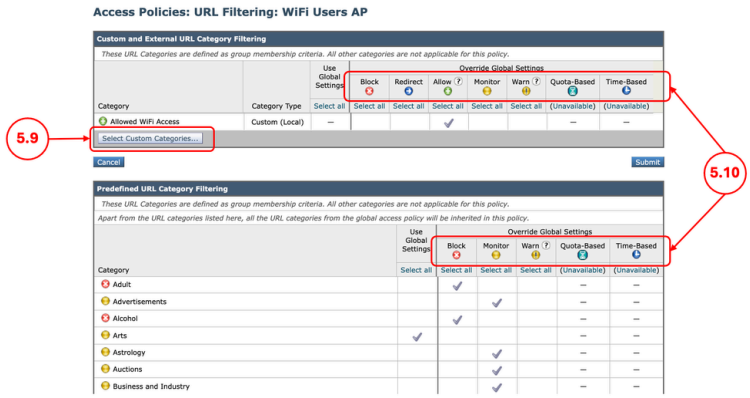


이미지 - 관리되는 디바이스에 대한 액세스 정책

5.8단계. Access Policies(액세스 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.

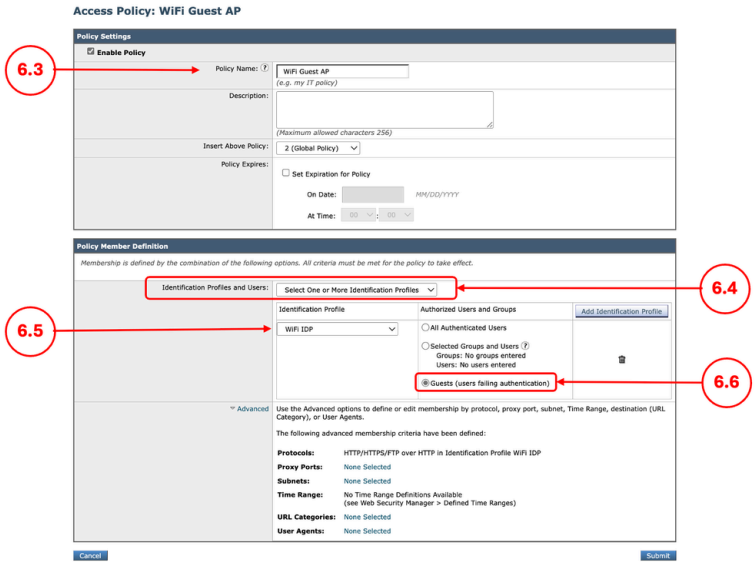
5.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다

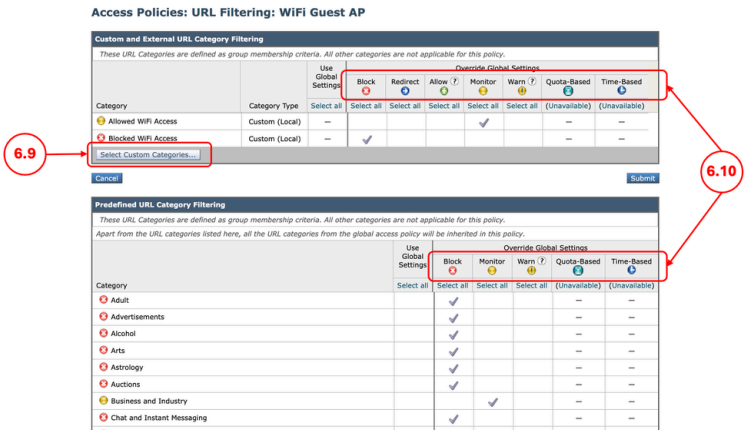
5.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링 및 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다.



이미지 - 관리되는 디바이스에 대한 액세스 정책 URL 필터링

5.11단계. Submit(제출)을 클릭합니다.

6단계. 관리되지 않는 디바이스에 대한 액세스 정책 생성	6.1단계. GUI에서 Web Security Manager로 이동하고 Access Policies(액세스 정책)를 선택합니다 6.2단계. Add Policy(정책 추가)를 클릭합니다. 6.3단계.새 정책의 EnterName을 입력합니다. 6.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다. 6.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다. 6.6단계. Guests(사용자 인증 실패)를 선택합니다. 6.7단계.Submit(제출)을 클릭합니다.  이미지 - 관리되지 않는 디바이스에 대한 액세스 정책 6.8단계. Access Policies(액세스 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다. 6.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다 6.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링 및 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다.



이미지 - 관리되지 않는 디바이스에 대한 액세스 정책 URL 필터링

6.11단계 Uncategorized URLs(분류되지 않은 URL) 섹션에서 아래로 스크롤하여 적절한 작업을 선택합니다.

이미지 - 액세스 정책 분류되지 않은 URL

팁: 보안 관점에서 URL에 액세스가 필요한 경우 정책에 할당된 사용자 지정 URL 카테고리에 작업을 Block(차단)으로 설정하는 것이 가장 좋습니다.

6.12단계. Submit(제출)을 클릭합니다.

7단계(선택 사항) 관리되는 디바이스에 대한 Cisco 데이터 보안 정책 생성

참고: 관리되는 디바이스에 대한 업로드 트래픽을 필터링하지 않으려면 이 단계를 건너뛸 수 있습니다.

7.1단계. GUI에서 Web Security Manager로 이동하고 Cisco Data Security를 선택합니다.

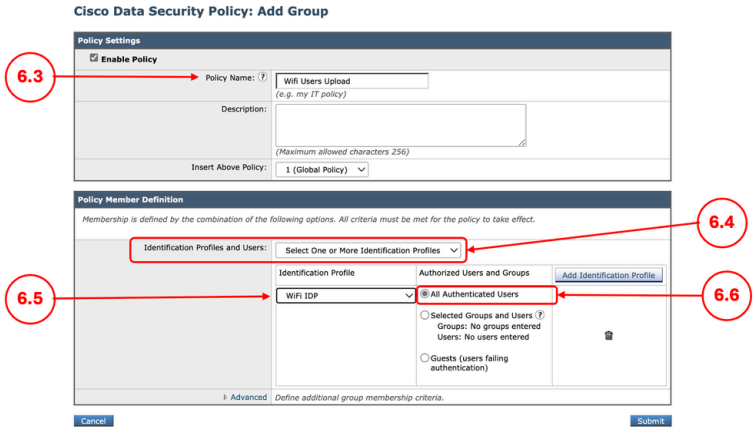
7.2단계. Add Policy(정책 추가)를 클릭합니다.

7.3단계.새 정책에 대한 EnterName을 입력합니다.

7.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다.

7.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다.

7.6단계. All Authenticated Users(인증된 모든 사용자)를 선택합니다.

	7.7단계.Submit(제출)을 클릭합니다.  이미지 - 관리되는 디바이스에 대한 Cisco 데이터 보안 정책 7.8단계. Cisco Data Security Policies(Cisco 데이터 보안 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다. 7.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다 7.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링과 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다.  이미지 - 관리되는 디바이스에 대한 업로드 작업 7.11단계. Submit(제출)을 클릭합니다.
8단계(선택 사항) 관리되지 않는 장치에 대한 Cisco 데이터 보안 정책을 생성합니다.	8.1단계. GUI에서 Web Security Manager로 이동하고 Cisco Data Security를 선택합니다. 8.2단계. Add Policy(정책 추가)를 클릭합니다.

참고: 관리되지 않는 디바이스에 대한 업로드 트래픽을 필터링하지 않으려면 이 단계를 건너뛸 수 있습니다.

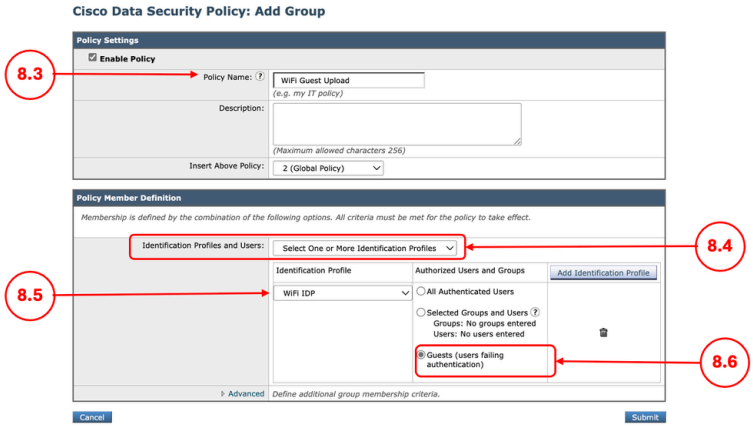
8.3단계.새 정책의 EnterName을 입력합니다.

8.4단계. Identification Profiles and Users(식별 프로필 및 사용자) 드롭다운 메뉴에서 Select One or More Identification Profiles(하나 이상 식별 프로필 선택)를 선택합니다.

8.5단계. 1단계에서 생성한 식별 프로파일을 선택합니다.

8.6단계. All Authenticated Users(인증된 모든 사용자)를 선택합니다.

8.7단계.Submit(제출)을 클릭합니다.

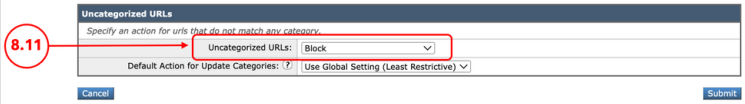


이미지 - 관리되지 않는 장치에 대한 Cisco 데이터 보안 정책

8.8단계. Cisco Data Security Policies(Cisco 데이터 보안 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.

8.9단계(선택 사항) Select Custom Categories(맞춤형 카테고리 선택)를 클릭하고 카테고리 이름 앞에서 Include in Policy(정책에 포함)를 선택하여 맞춤형 URL 카테고리를 추가할 수 있습니다

8.10단계. 각 맞춤형 및 외부 URL 카테고리 필터링과 미리 정의된 URL 카테고리 필터링에 대한 작업을 구성합니다.

	 이미지 - 관리되지 않는 디바이스에 대한 업로드 작업 8.11단계 Uncategorized URLs(분류되지 않은 URL) 섹션에서 아래로 스크롤하여 적절한 작업을 선택합니다.  이미지 - 분류되지 않은 URL에 대한 업로드 작업 팁: 보안 관점에서 URL에 액세스가 필요한 경우 정책에 할당된 사용자 지정 URL 카테고리에 작업을 Block(차단)으로 설정하는 것이 가장 좋습니다. 8.12단계. Submit(제출)을 클릭합니다.
9단계. 변경 사항 저장	9.1단계. 변경 사항 커밋

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance - LD 사용 설명서(제한적 배포) - 문제 해결 방법...
- SWA에서 실행 파일 다운로드 차단
- Secure Web Appliance에서 업로드 트래픽 차단
- Secure Web Appliance에서 트래픽 차단
- Secure Web Appliance에서 인증 우회
- SWA에서 Microsoft O365 테넌트 제한 구성
- Secure Web Appliance 초기 설정 구성
- 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.