Secure Web Appliance에서 인증 우회

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[제외 인증](#)

[Cisco SWA에서 인증을 면제 하는 방법](#)

[인증 우회 단계](#)

[관련 정보](#)

소개

이 문서에서는 SWA(Secure Web Appliance)에서 인증을 면제하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.

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.

제외 인증

Cisco SWA에서 특정 사용자 또는 시스템에 대한 인증을 면제하는 것은 운영 효율성을 유지하고 특정 요구 사항을 충족하는 데 매우 중요할 수 있습니다. 첫째, 일부 사용자 또는 시스템은 인증 프로세스로 인해 방해가 될 수 있는 중요한 리소스 또는 서비스에 대한 무중단 액세스를 필요로 합니다.

예를 들어, 정기적인 업데이트 또는 백업을 수행하는 자동화된 시스템 또는 서비스 계정은 인증 메커니즘으로 인한 지연 또는 잠재적 오류 없이 원활한 액세스가 필요합니다.

또한 웹 서비스 공급자가 서비스에 액세스하기 위해 프록시를 사용하지 않도록 권장하는 시나리오도 있습니다. 이러한 경우 인증을 면제하면 사업자 지침을 준수하고 서비스 신뢰도를 유지할 수 있습니다. 또한 특정 사용자의 트래픽을 효과적으로 차단하려면 먼저 인증을 면제하고 적절한 차단 정책을 적용해야 하는 경우가 많습니다. 이러한 접근 방식을 통해 액세스 권한을 정밀하게 제어할 수 있습니다.

Microsoft 업데이트와 같이 액세스 중인 웹 서비스를 신뢰할 수 있고 보편적으로 수용할 수 있는 경우도 있습니다. 이러한 서비스에 대한 인증을 면제하면 모든 사용자의 액세스가 간소화됩니다. 또한 사용자 운영 체제 또는 애플리케이션이 SWA에서 구성된 인증 메커니즘을 지원하지 않아 연결을 보장하기 위해 우회가 필요한 경우가 있습니다.

마지막으로, 사용자 로그인이 없고 신뢰할 수 있는 인터넷 액세스가 제한된 고정 IP 주소를 사용하는 서버는 액세스 패턴이 예측 가능하고 안전하므로 인증이 필요하지 않습니다.

이러한 경우에 대한 인증을 전략적으로 면제함으로써 조직은 보안 요구와 운영 효율성의 균형을 맞출 수 있습니다.

Cisco SWA에서 인증을 면제 하는 방법

SWA에서 인증 면제는 다양한 방법을 통해 달성할 수 있으며, 각 방법은 특정 시나리오 및 요구 사항에 맞게 조정됩니다. 인증 면제를 구성하는 몇 가지 일반적인 방법은 다음과 같습니다.

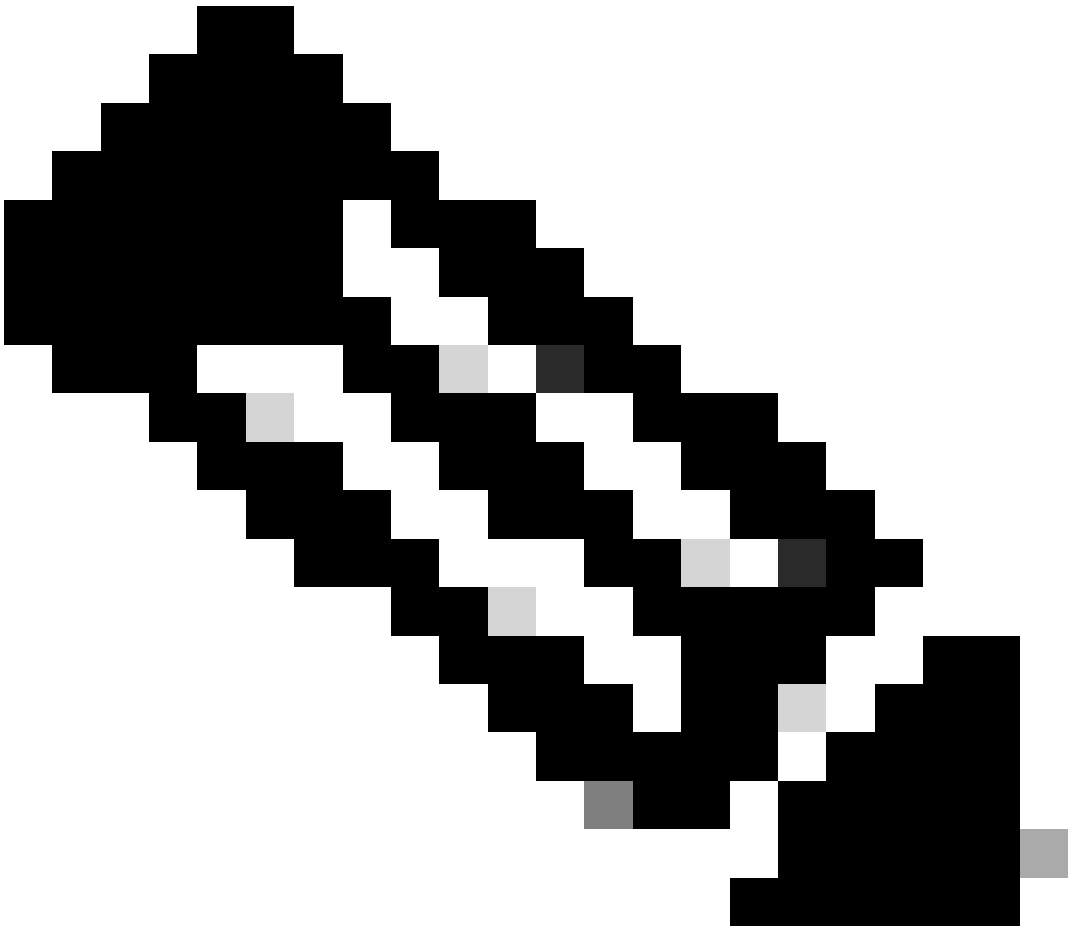
- IP 주소 또는 서브넷 마스크: 가장 간단한 방법 중 하나는 특정 IP 주소 또는 전체 서브넷을 인증에서 제외하는 것입니다. 이 기능은 인터넷 또는 내부 리소스에 대한 무중단 액세스가 필요한 고정 IP 주소 또는 신뢰할 수 있는 네트워크 세그먼트를 가진 서버에 특히 유용합니다. SWA 컨피그레이션에서 이러한 IP 주소 또는 서브넷 마스크를 지정하여 이러한 시스템이 인증 프로세스를 우회하도록 할 수 있습니다.
- 프록시 포트: 특정 프록시 포트를 기반으로 트래픽을 제외하도록 SWA를 구성할 수 있습니다. 이는 특정 애플리케이션 또는 서비스가 통신을 위해 지정된 포트를 사용할 때 유용합니다. 이러한 포트를 식별하여 해당 포트의 트래픽에 대한 인증을 우회하도록 SWA를 설정하여 관련 애플리케이션 또는 서비스에 대한 원활한 액세스를 보장할 수 있습니다.
- URL 범주: 또 다른 방법은 URL 범주에 따라 인증을 면제하는 것입니다. 여기에는 미리 정의된 Cisco 범주 및 조직별 요구 사항에 따라 정의하는 맞춤형 URL 범주가 모두 포함될 수 있습니다. 예를 들어 Microsoft 업데이트와 같은 특정 웹 서비스가 신뢰할 수 있고 보편적으로 허용되는 것으로 간주되는 경우 이러한 특정 URL 범주에 대한 인증을 우회하도록 SWA를 구성할 수 있습니다. 이렇게 하면 모든 사용자가 인증 없이 이러한 서비스에 액세스할 수 있습니다.
- 사용자 에이전트: 사용자 에이전트를 기준으로 인증을 제외하는 것은 구성된 인증 메커니즘을 지원하지 않는 특정 애플리케이션 또는 디바이스를 다룰 때 유용합니다. 이러한 애플리케이션 또는 디바이스의 사용자 에이전트 문자열을 식별하여, 그로부터 시작되는 트래픽에 대한 인증을 우회하도록 SWA를 구성하여 원활한 연결을 보장할 수 있습니다.

.

인증 우회 단계

인증에서 제외할 식별 프로필을 생성하는 단계는 다음과 같습니다.

1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다.
2단계. 프로필을 추가하려면 Add Profile을 클릭합니다.
3단계. 이 프로파일을 활성화하거나 삭제하지 않고 신속하게 비활성화하려면 Enable Identification Profile 확인란을 사용합니다.
4단계. 고유한 프로파일 이름을 할당합니다.
5단계. (선택 사항) 설명을 추가합니다.
6단계. Insert the 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다.

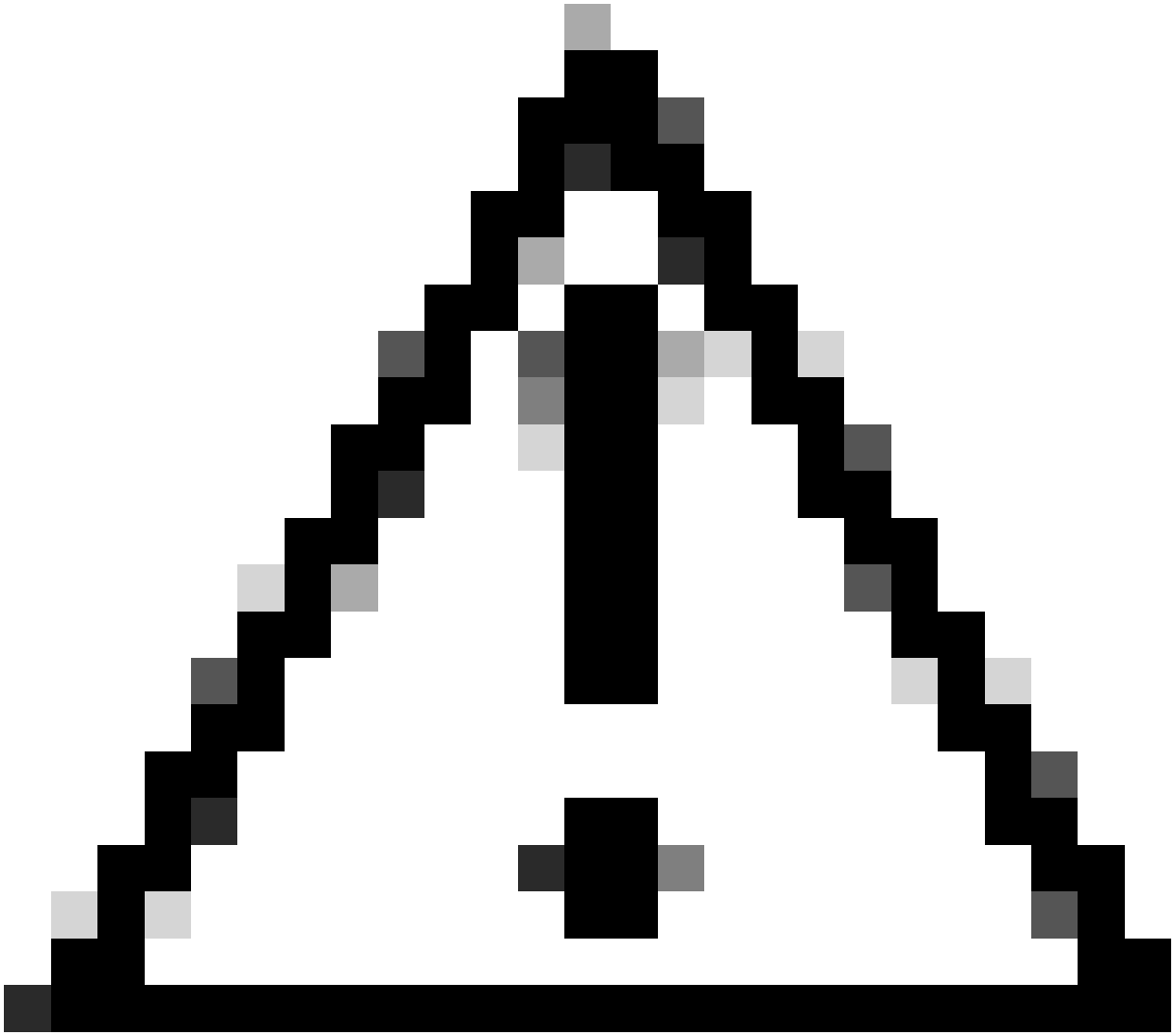


참고: 인증이 필요하지 않은 ID 프로파일을 목록의 맨 위에 배치합니다. 이 접근 방식은 SWA에 대한 부하를 줄이고, 인증 대기열을 최소화하며, 다른 사용자의 인증 속도를 높입니다.

7단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다.

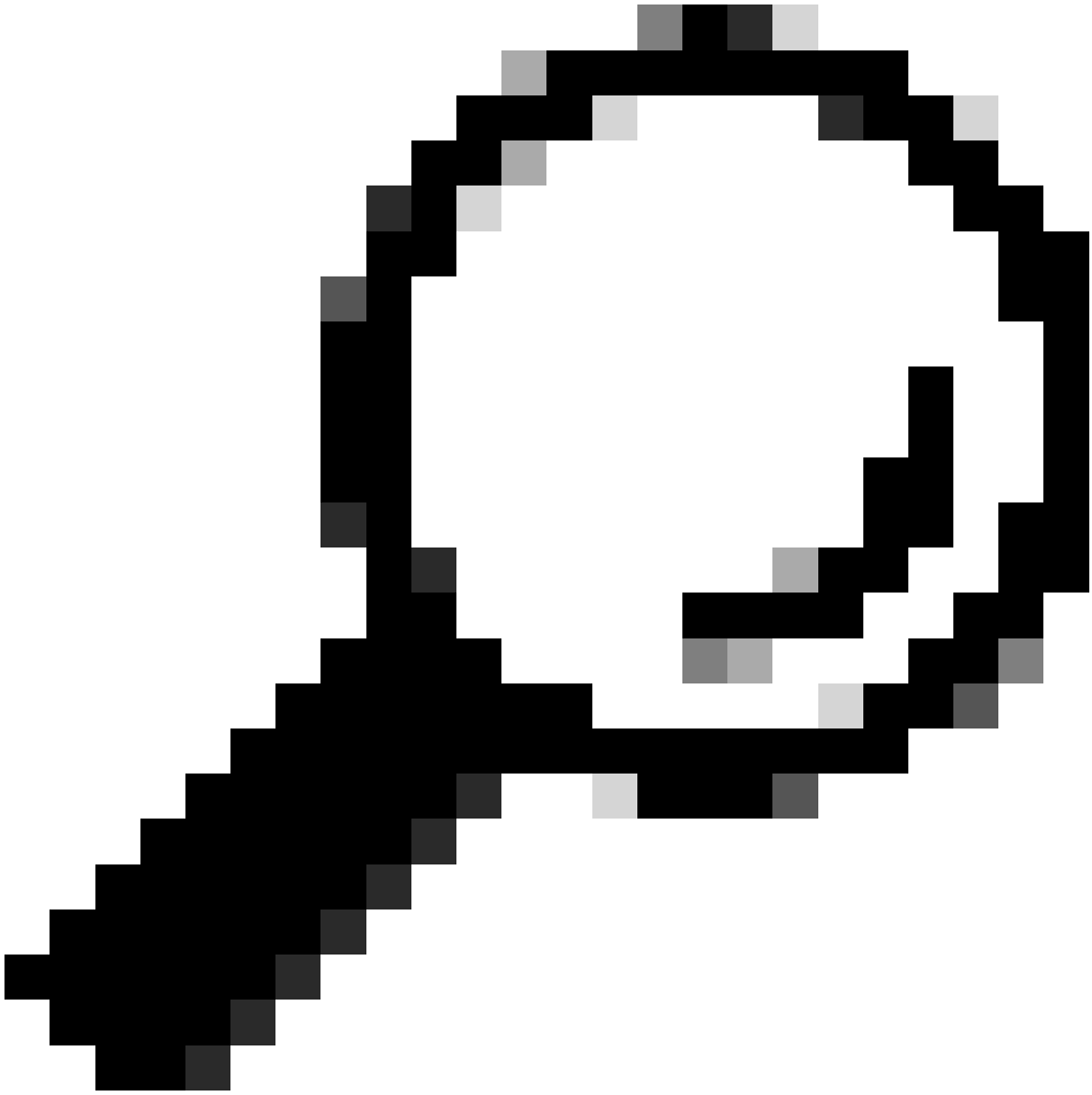
8단계. 서브넷별 구성원 정의에 이 식별 프로필이 적용해야 하는 IP 주소 또는 서브넷을 입력합니다. IP 주소, CIDR(Classless Inter-Domain Routing) 블록 및 서브넷을 사용할 수 있습니다.

9단계(선택 사항) Advanced(고급)를 클릭하여 Proxy Ports(프록시 포트), URL Categories(URL 카테고리) 또는 User Agents(사용자 에이전트)와 같은 추가 구성원 기준을 정의합니다자가를 선택합니다.

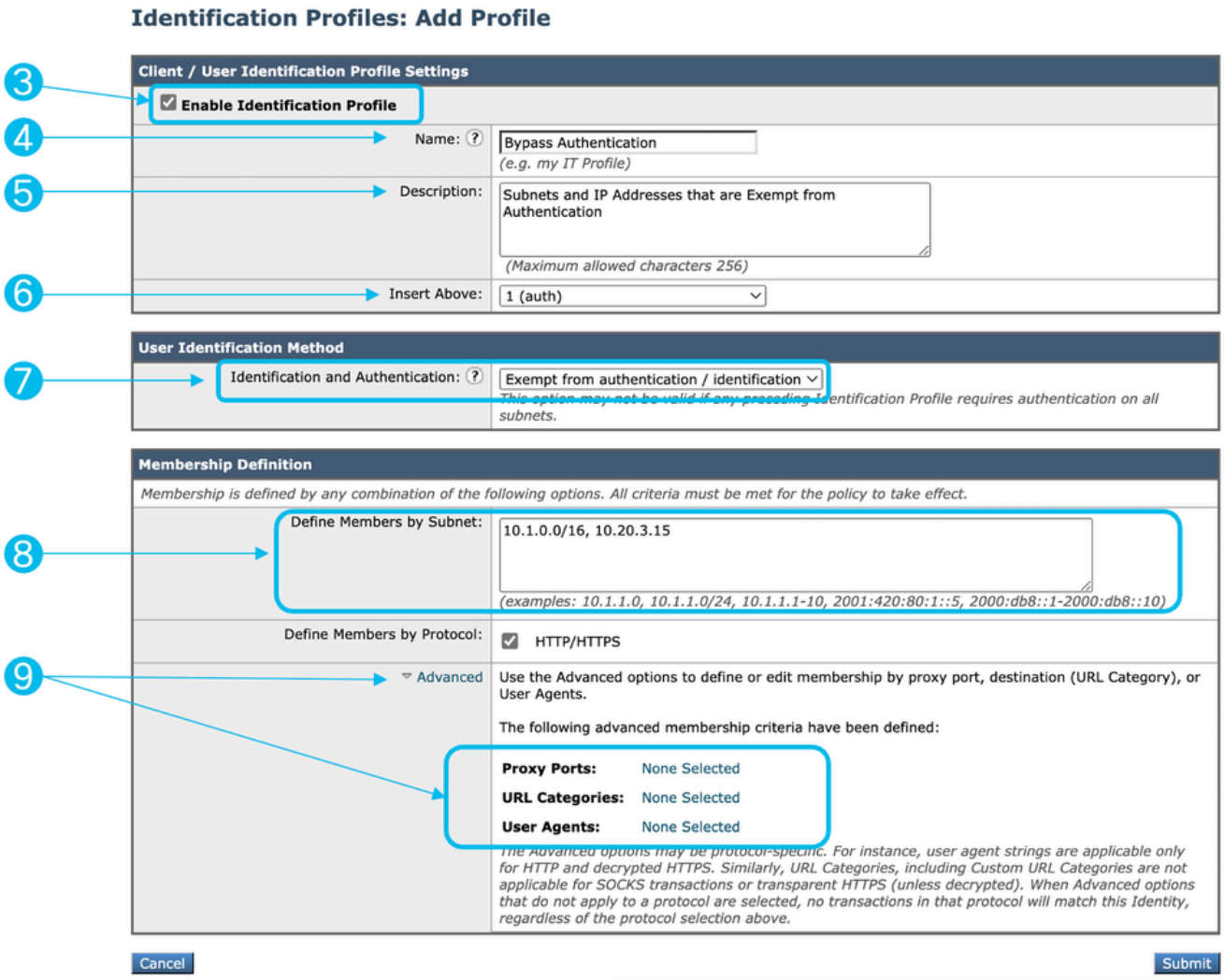


주의: 투명 프록시 구축에서 SWA는 트래픽이 해독되지 않는 한 HTTPS 트래픽에 대한 사용자 에이전트 또는 전체 URL을 읽을 수 없습니다. 따라서 User Agents(사용자 에이전트)를 사용하여 식별 프로필을 구성하거나 정규식과 함께 Custom URL Category(맞춤형 URL 카테고리)를 구성하는 경우 이 트래픽은 식별 프로필과 매칭하지 못합니다.

맞춤형 URL 카테고리 구성 방법에 대한 자세한 내용은 Secure Web Appliance에서 맞춤형 URL 카테고리 구성 - Cisco를 참조하십시오.



팁: 정책에서는 AND 논리를 사용하므로 ID 프로파일이 일치하려면 모든 조건을 충족해야 합니다. 고급 옵션이 설정된 경우 정책이 적용되려면 모든 요구 사항이 충족되어야 합니다.



이미지 - ID 프로필을 생성하여 인증을 우회하는 단계

10단계. 변경 사항을 제출하고 커밋합니다.

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서 - GD(일반 배포) - 정책 애플리케이션 최종 사용자 분류 [Cisco Secure Web Appliance] - Cisco
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
- Cisco WSA(Web Security Appliance)에서 Office 365 트래픽을 인증 및 암호 해독에서 제외하는 방법 - 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.