SWA에서 실행 파일 다운로드 차단

목차

소개

이 문서에서는 실행 파일 다운로드를 차단하도록 SWA(Secure Web Appliance)를 구성하는 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.

시작하기 전에

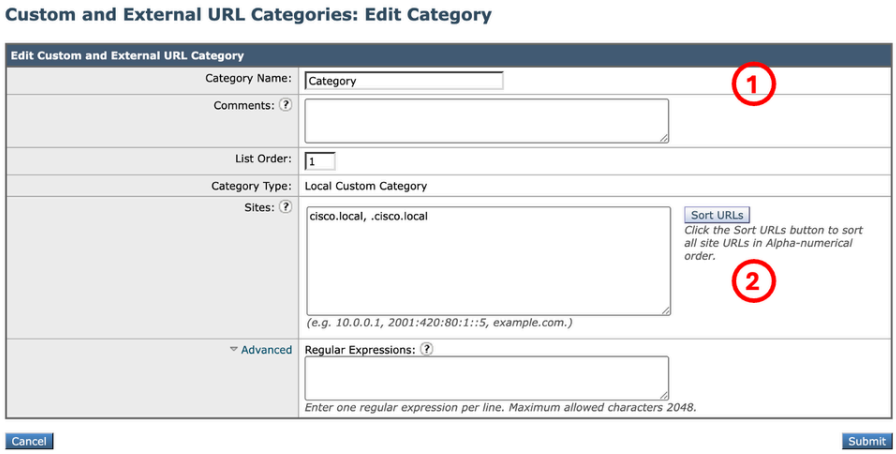
Cisco SWA는 웹 콘텐츠의 (Multipurpose Internet Mail Extensions) MIME 유형을 검사하여 실행 파일의 다운로드를 효과적으로 차단할 수 있습니다. SWA는 application/x-msdownload, application/x-msi 및 기타 관련 MIME 유형과 같은 파일 유형을 식별하여 실행 파일이 사용자에게 전달되지 않도록 하는 정책을 적용합니다. MIME 유형 탐지 외에도 SWA는 파일 확장자 필터링, 평판 기반 분석, 사용자 지정 정책 규칙을 활용하여 원치 않는 다운로드 또는 위험한 다운로드에 대한 보호를 더욱 강화할 수 있습니다. 이러한 기능을 통해 조직은 안전한 검색 환경을 유지하고 악성코드 감염의 위

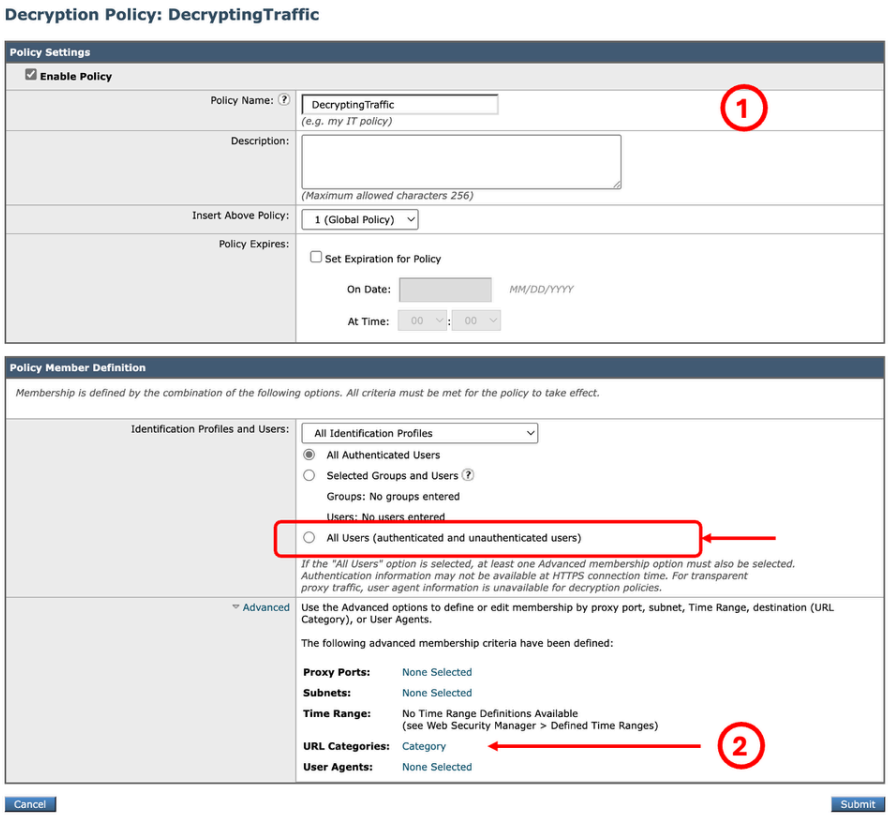
험을 줄일 수 있습니다.

팁: 트래픽이 해독되지 않는 한 SWA는 파일의 MIME 유형을 식별할 수 없습니다.

application/octet-stream은 파일에 이진 데이터가 포함되어 있음을 나타내는 데 사용되는 일반 MIME 형식입니다. 파일의 특성을 지정하지 않으므로 보다 구체적인 MIME 유형에 맞지 않는 파일에 사용할 수 있습니다. 이 형식은 일반적으로 실행 파일, 설치 프로그램 및 기타 텍스트가 아닌 파일에 할당되며, 웹 서버에서 더 정확한 형식을 확인할 수 없습니다.

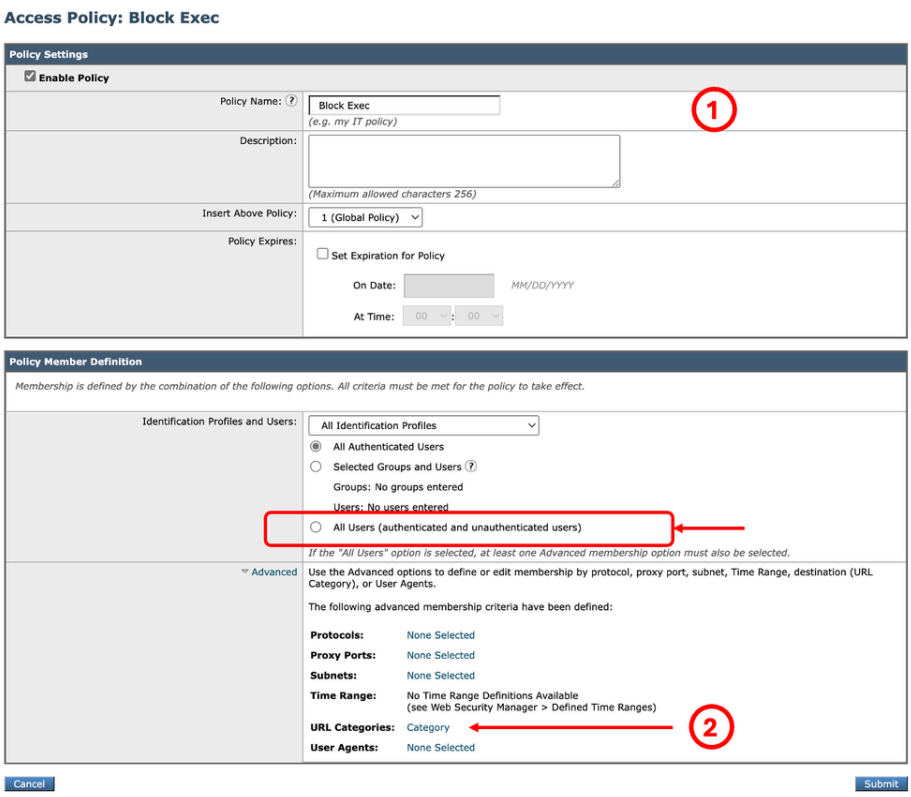
컨피그레이션 단계

1단계.웹 사이트에 대한 사용자 지정 URL 카테고리를 생성합니다.	1.1단계.GUI에서 Web Security Manager로 이동하고 Custom and External URL Categories(사용자 지정 및 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.local 및 모든 하위 도메인). 1.5단계.변경 내용을 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-cu를 참조하십시오.

2단계.URL의 트래픽을 해독합니다.	⚠ 주의: 많은 URL의 암호를 해독하면 성능이 저하될 수 있습니다. 2.1단계. GUI에서 Web Security Manager로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다 2.2단계. Add Policy(정책 추가)를 클릭합니다. 2.3단계. 새 정책의 EnterName을 입력합니다. 2.4단계(선택 사항) 이 정책을 적용할 식별 프로필을 선택합니다. 팁: (선택 사항) 인증되지 않은 모든 사용자에 대해 정책을 적용하려면 All Users(Authenticated 및 Unauthenticated users)를 선택합니다. 2.5단계.Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리)Links(링크)를 클릭하여 사용자 지정 URL 카테고리를 추가합니다. 2.6단계.1단계에서 생성한 URL 카테고리를 선택합니다. 2.7단계.Submit(제출)을 클릭합니다.  이미지 - 암호 해독 정책 생성

	2.8단계Decryption Policies(암호 해독 정책) 페이지에서 새 정책에 대한 URL Filtering(URL 필터링)의 링크를 클릭합니다. **Decryption Policies** **Policies** Add Policy... 	Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
---	---	---	---	---	---	---
1	**DecryptingTraffic** Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		| Edit Policy Order... 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. **Decryption Policies: URL Filtering: DecryptingTraffic** **Custom and External URL Category Filtering** *These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.* | Category	Category Type	Use Global Settings	Override Global Settings: Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
---	---	---	---	---	---	---	---	---
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Category	Custom (Local)	–			✓		–	–	 Cancel Submit Image(이미지) - Set Decrypt as Action(해독을 작업으로 설정)
3단계.실행 파일 차단	3.1단계.GUI에서 Web Security Manager로 이동하고 Access Policies(액세스 정책)를 선택합니다. 3.2단계.[정책 추가]를 클릭합니다. 3.3단계. 새 정책의 EnterName을 입력합니다. 3.4단계(선택 사항) 이 정책을 적용할 식별 프로필을 선택합니다. 팁: (선택 사항) 인증되지 않은 모든 사용자에 대해 정책을 적용하려면 All Users(Authenticated 및 Unauthenticated users)를 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 - 액세스 정책

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

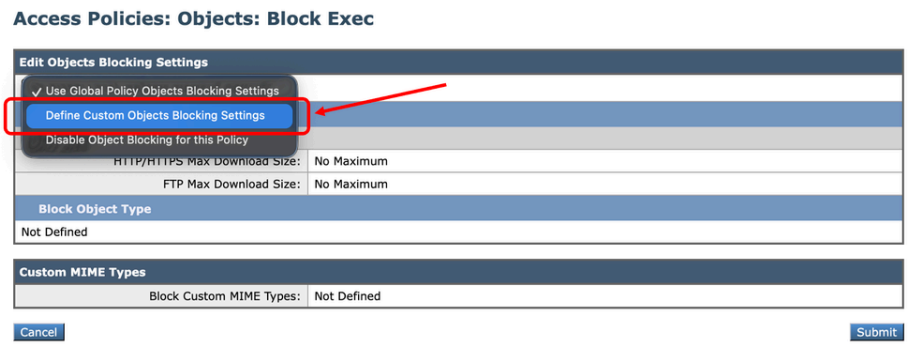
3.8단계.InAccess Policies(액세스 정책) 페이지에서 URL 필터링 작업이 Monitor(모니터링)로 설정되어 있는지 확인합니다.

3.9단계. Access Policies(액세스 정책) 페이지에서 새 정책에 대한 Objects(개체)의 링크를 클릭합니다.

이미지 - 객체 선택

이미지 - URL 필터링 선택

3.10단계. 드롭다운 메뉴에서 Define Custom Objects Blocking Settings를 선택합니다.

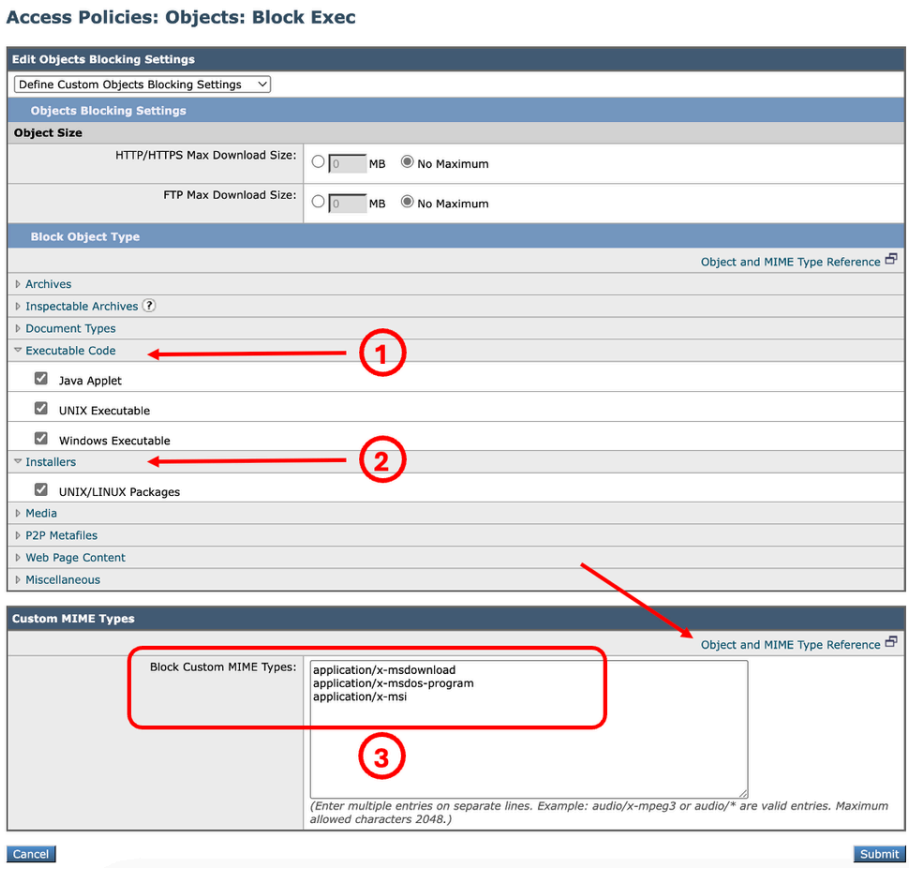


이미지 - 사용자 지정 개체 정의

3.11단계.차단할 개체 유형을 선택하려면 실행 코드를 클릭합니다.

3.12단계.Installers(설치 프로그램)를 클릭하여 차단할 개체 유형을 선택합니다.

3.13단계. 또한 Custom MIME Types(사용자 지정 MIME 유형) 섹션에서 차단할 파일의 MIME 유형을 입력할 수 있습니다.

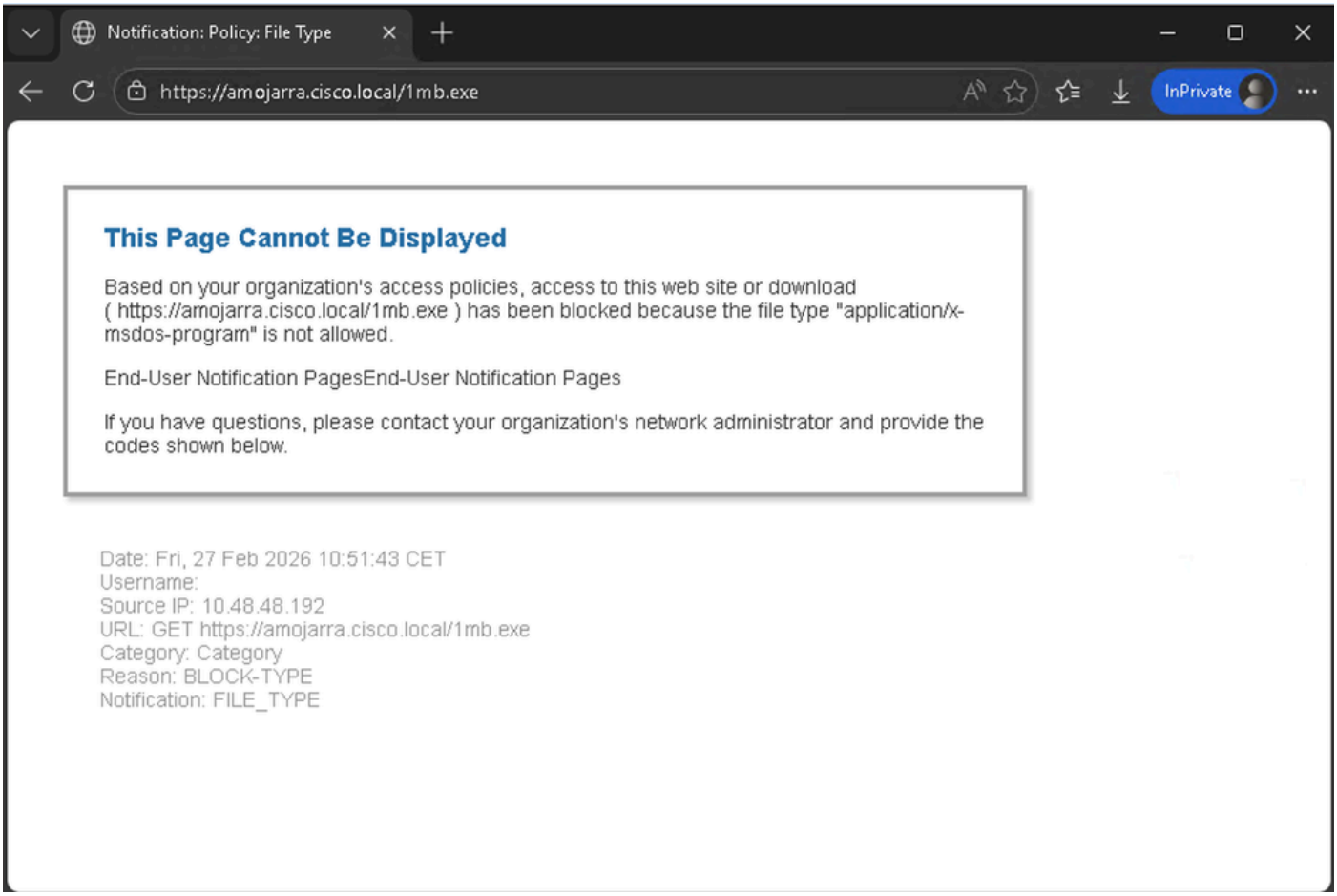


이미지 - 차단할 객체 구성

	팁: MIME 유형의 목록을 보려면 Object and MIME Type Reference를 클릭합니다. 3.14단계.제출. 3.15단계.변경 사항을 커밋합니다.

파일 확장명 차단 검증

이 예에서는 사용자가 실행 파일을 다운로드하려고 하면 다음 경고 페이지가 표시됩니다.



이미지 - 차단 알림 페이지

팁: EUN(End User Notification) 페이지를 구성하려면 GUI에서 Security Services(보안 서비스)로 이동하여 End-User Notification(최종 사용자 알림)을 클릭하고 End-User Notification Pages(최종 사용자 알림 페이지) 섹션을 수정합니다.

액세스 로그에서는 트래픽과 관련된 두 개의 로그 행을 볼 수 있습니다.

첫 번째 로그 라인은 암호 해독 정책과 관련이 있습니다(이름: 트래픽 해독)을 참조하십시오. 작업은 DECRYPT_CUSTOMCAT입니다

두 번째 액세스 로그 라인은 액세스 정책(이름: Block_Exec). 3 단계에서 생성한 작업입니다. 작업은 BLOCK_ADMIN_FILE_TYPE입니다.

정책	액세스 로그
암호 해독 정책	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-NONE-LAB_Access-NONE <"C_C cate",-,"-",-,-,-,-,"-",-,-,"-",-","-,",-","-","-","-","-","-","-","-","-","-","-","-","-,"-",-,"-,-,"-,-,"-,"-,"-,"-,","-,"-,",-,-,"-,-,-> - -
액세스 정책	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_C cate",ns,0,"-",0,0,0,-,"-",-,-,-",-",-",-,-,"nc",-,"-","-","-","알 수 없음","알 수 없음","-","-",",0.00,0,-,"알 수 없음","-",-,"-,"-",-,-",-,-,"-,"-,-,-> -

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.