SWA에서 Kerberos Single-Sign-On 인증 구성

목차

소개

이 문서에서는 프록시 사용자가 SWA(Secure Web Appliance)에서 Kerberos를 통한 SSO(Single-Sign-On) 인증을 갖도록 구성하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.
- 기본 Active Directory 관리.

Cisco에서는 다음과 같은 툴을 설치하는 것이 좋습니다.

- 물리적 또는 가상 SWA.

- SWA GUI(Graphical User Interface)에 대한 관리 액세스
- Active Directory에 대한 관리 액세스

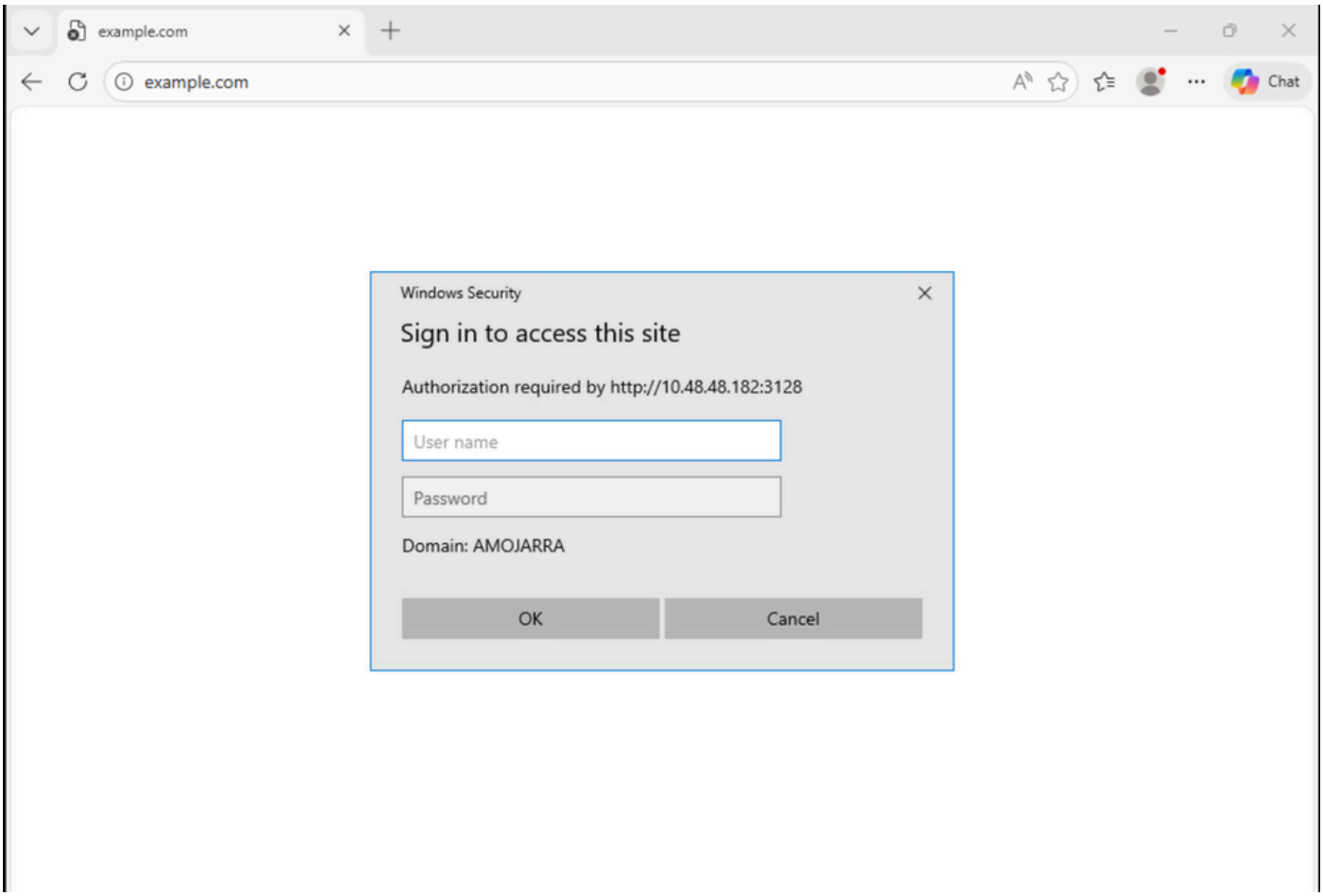
사용되는 구성 요소

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

프록시 클라이언트가 웹 사이트에 액세스를 시도하고 자격 증명을 수동으로 입력하라는 메시지가 표시되면 다음 단계를 사용하여 문제를 해결합니다.



이미지 - 사용자 인증 프롬프트

1단계. 클라이언트와 관련된 Accesslogs(액세스 로그)를 확인합니다.

1.1단계. CLI에 로그인합니다.

1.2단계. grep를 실행합니다.

1.3단계. 와 연관된 번호를 선택합니다. 액세스 로그.

1.4단계. Enter the regular expression to grep(grep 정규식을 입력하여 클라이언트 IP 주소)에 입력합니다.

1.5단계. Do you want to tail the logs(로그를 테일링하시겠습니까?)가 표시될 때까지 Enter 키를 누르고 "Y"를 입력한 다음 Accesslogs(액세스 로그)가 표시될 때까지 Enter 키를 누릅니다.

1.6단계. 클라이언트 PC에서 웹 사이트에 액세스하여 문제를 다시 생성합니다.

1.7단계. 트래픽이 도달하고 있는 식별 프로필을 확인합니다.

이 예에서 식별 프로필은 Auth_ID입니다.

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

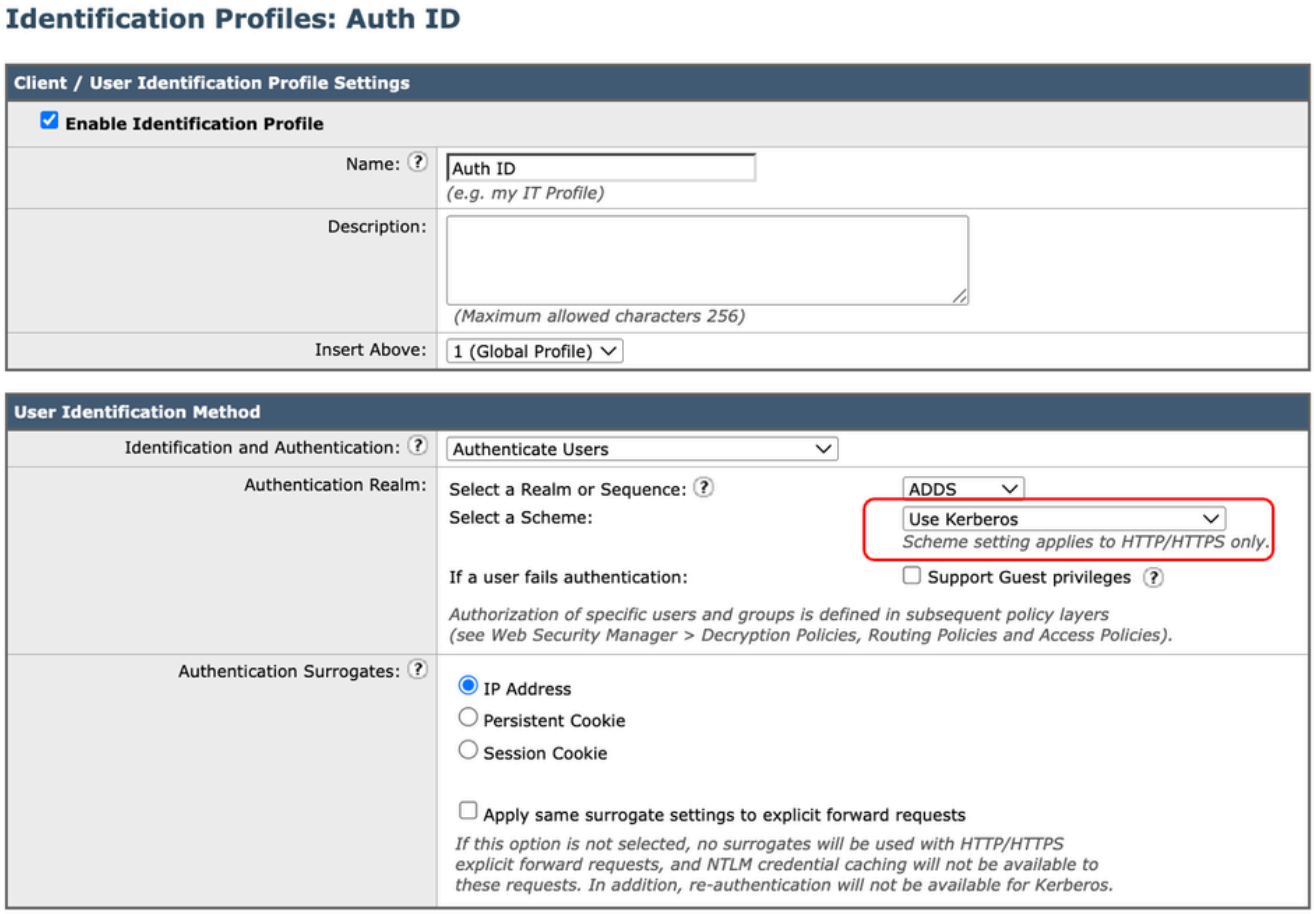
2단계. 식별 프로필을 확인합니다.

2.1단계. SWA의 GUI에 로그인합니다.

2.2단계. Web Security Manager에서 Identification Profiles(식별 프로필)를 선택합니다.

2.3단계. 트래픽이 발생한 식별 프로필의 이름을 클릭합니다.

2.4단계. Authentication Scheme(인증 체계)이 Basic(기본)으로 설정되어 있지 않은지 확인합니다.



이미지 - 인증 스키마

3단계. SWA 및 Active Directory 연결을 테스트합니다.

3.1단계. SWA GUI에서 Network(네트워크)로 이동하고 Authentication(인증)을 선택합니다.

3.2단계. 인증 영역 이름을 클릭합니다.

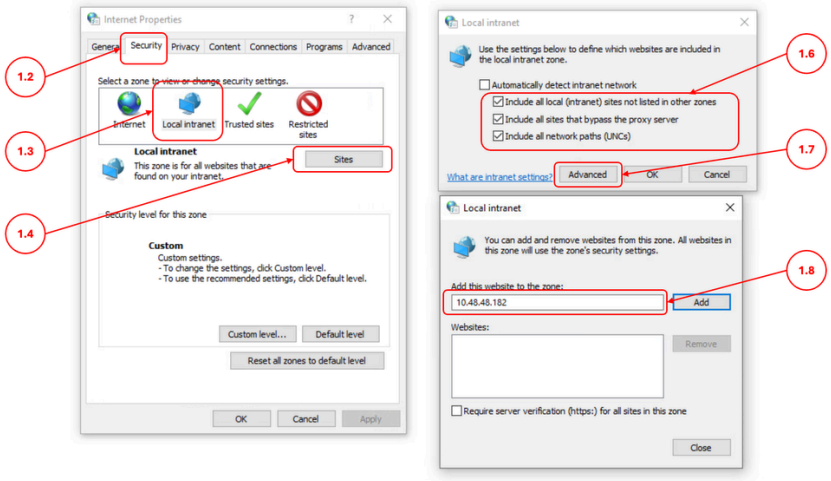
3.3단계. Start Test(테스트 시작)를 클릭하여 SWA 및 Active Directory 연결 상태를 검토합니다.

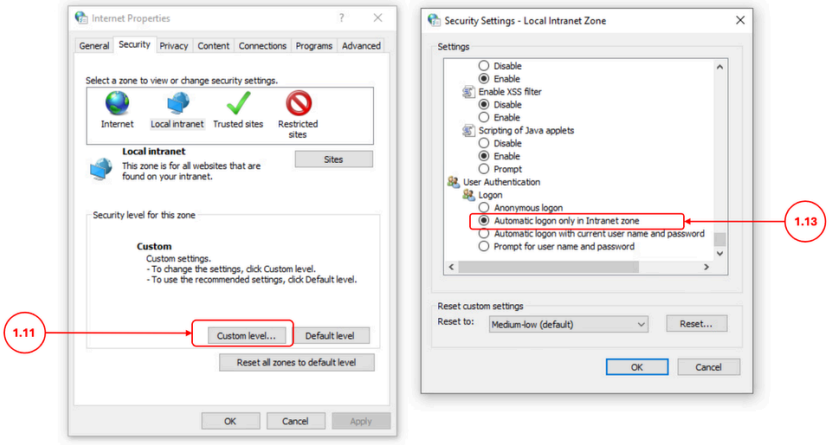
오류가 발견되지 않으면 이 문서에 설명된 대로 클라이언트 PC 컨피그레이션을 확인합니다.

클라이언트 PC 구성

다음 단계를 사용하여 클라이언트 PC 컨피그레이션을 확인합니다.

단계	세부사항

1단계. 로컬 인트라넷 사이트	1.1단계. 시작 메뉴에 인터넷 옵션을 입력하고 Enter 키를 누릅니다. 1.2단계. 인터넷 속성 창에서 보안 탭을 클릭합니다. 1.3단계. Local Intranet(로컬 인트라넷)을 선택합니다. 1.4단계. 사이트를 클릭합니다. 1.5단계. 자동으로 인트라넷 네트워크 검색 확인란이 선택되지 않았는지 확인합니다. 1.6단계. 다음 세 가지 옵션을 모두 선택합니다. • 다른 영역에 나열되지 않은 모든 로컬(인트라넷) 사이트 포함 • 프록시 서버를 우회하는 모든 사이트 포함 • 모든 네트워크 경로 포함(UNC) 1.7단계. Advanced(고급)를 클릭합니다. 1.8단계. SWA의 FQDN 또는 IP 주소를 입력하고 목록에 Add(추가)를 입력합니다. 1.9단계(선택 사항) 내부 보안 정책에 따라 Require Server Verification(서버 확인 필요)을 비활성화할 수 있습니다.  이미지 - 로컬 Interanet 사이트 구성 1.10단계. 닫기 및 확인을 클릭합니다. 1.11단계. Security(보안) 탭에서 Custom level(사용자 지정 레벨)을 클릭합니다. 1.12단계. 사용자 인증으로 스크롤합니다. 1.13단계. 인트라넷 영역에서만 자동 로그온을 선택합니다.

	 이미지 - 인트라넷 사용자를 위한 자동 로그인
2단계. 로그 수집	1단계에서 Kerberos를 통해 SSO 인증을 수정하지 않은 경우 2.1단계. SWA 인증 로그를 Trace(추적)로 변경하고 로그를 검토합니다. 2.2단계. [Auth-Method = %m]을(를) 액세스 로그에 사용자 지정 필드로 추가합니다. 자세한 내용은 다음 사이트를 참조하십시오. 액세스 로그에서 성능 매개변수를 구성합니다. 2.3단계. 클라이언트 IP 및 Active Directory IP 주소에 대한 패킷 캡처 필터를 실행하고 클라이언트 PC가 Kerberos 서비스 티켓을 SWA로 전송하는지 확인합니다.

참고: 브라우저 프록시 설정에서 SWA의 FQDN을 구성했는지 확인하십시오.

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서
- Secure Web Appliance용 방화벽 구성
- Content Security Appliance에서 패킷 캡처 구성
- 액세스 로그의 성능 매개변수 구성
- Secure Web Appliance 로그 액세스
- Use Secure Web Appliance 모범 사례 - Cisco
- Secure Web Appliance에서 인증 우회 - 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.