Cisco Secure Firewall에서 Zero Trust 액세스를 사용하여 애플리케이션을 보호하는 방법

초판: 2024년 1월 29일

Zero Trust 네트워크 액세스 개요

Zero Trust 액세스는 각 네트워크 액세스 시도에 대한 지속적인 인증 및 모니터링을 통해 신뢰를 설정하는 보안 모델을 기반으로 합니다. Secure Firewall Management Center 웹 인터페이스를 사용하여 ZTA(Zero Trust 애플리케이션) 정책을 생성하고 위협 정책을 할당할 수 있는 Zero Trust Application Policy(Zero Trust 애플리케이션 정책)을 생성할 수 있습니다. 이 정책은 애플리케이션별, 즉 관리자가 해당 애플리케이션에 대한 위협 인식에 따라 검사 수준을 결정합니다.

이 문서에서는 애플리케이션을 보호하고 위협 및 악성코드 방지를 구현하는 전체 프로세스를 보여주는 시나리오를 간략하게 설명합니다. 이 문서에는 애플리케이션에 액세스하고, 위협 및 악성코드로부터 애플리케이션을 보호하고, Zero Trust 세션을 모니터링하는 유효성 검사 단계도 포함되어 있습니다.

Secure Firewall Management Center에서 Zero Trust 액세스 기능

- Duo, Microsoft Azure Active Directory, Okta 등 여러 SAML 기반 ID 제공자를 지원합니다.
- 보안 액세스를 위해 엔드포인트(클라이언트 디바이스)에서 Cisco AnyConnect과 같은 애플리케이션.
- 브라우저를 통한 액세스 및 인증을 지원합니다.
- 웹 애플리케이션(HTTPS)만 지원합니다.
- Duo의 정책으로 디바이스의 상태를 평가하고 평가에 따라 액세스를 제공할 수 있는 Duo Health와 같은 에이전트를 통해 클라이언트 디바이스 상태를 지원합니다. 서드파티 ID 공급업체와 함께 동일한 기능을 수행하여 에이전트와 함께 상태 평가를 지원할 수 있습니다.
- HTTP 리디렉션 SAML 바인딩을 지원합니다.
- 애플리케이션 그룹을 지원하여 애플리케이션 집합에서 Zero Trust 보호를 쉽게 활성화할 수 있습니다.
- Zero Trust 애플리케이션 트래픽에서 Threat Defense 침입 및 악성코드 보호를 활용합니다.

Zero Trust 액세스 사용을 위한 사전 요건

이 문서에서는 Zero Trust 개념에 대한 기본 사항을 이해하고 있으며 Cisco Secure Firewall Management Center 디바이스 구성 가이드버전 7.4 이상의 "Zero Trust 액세스" 장을 완료했다고 가정합니다.

이 활용 사례가 귀사에 적합합니까?

이 활용 사례에서는 클라이언트리스 Zero Trust 네트워크 액세스 모델을 사용하여 프라이빗 애플리케이션 및 리소스에 액세스하는 프로세스를 간략하게 설명합니다. 클라이언트 기반 보안 네트워크 및 애플리케이션 액세스에는 Cisco Secure Client를 사용하는 것이 좋습니다. 자세한 내용은 Cisco Secure Client를 참조하십시오.

이 활용 사례는 Secure Firewall Management Center에서 Zero Trust 기능을 사용하여 하이브리드 워크포스가 보호되는 리소스 및 웹 애플리케이션에 액세스할 수 있도록 지원하고, 보호되는 리소스 및 애플리케이션을 악성코드로부터 보호하는 것을 목표로 합니다.

Zero Trust 액세스 구현 시나리오

직원과 계약업체가 다양한 위치에서 근무하고 회사 방화벽 뒤에서 호스팅되는 프라이빗 애플리케이션 및 리소스에 액세스하는 인력이 분산된 대규모 엔터프라이즈가 있습니다. 관리자는 직원이 보호되는 애플리케이션에 액세스할 때 악의적인 활동을 수행하는 것을 방지하고자 합니다.

어떤 위험이 있습니까?

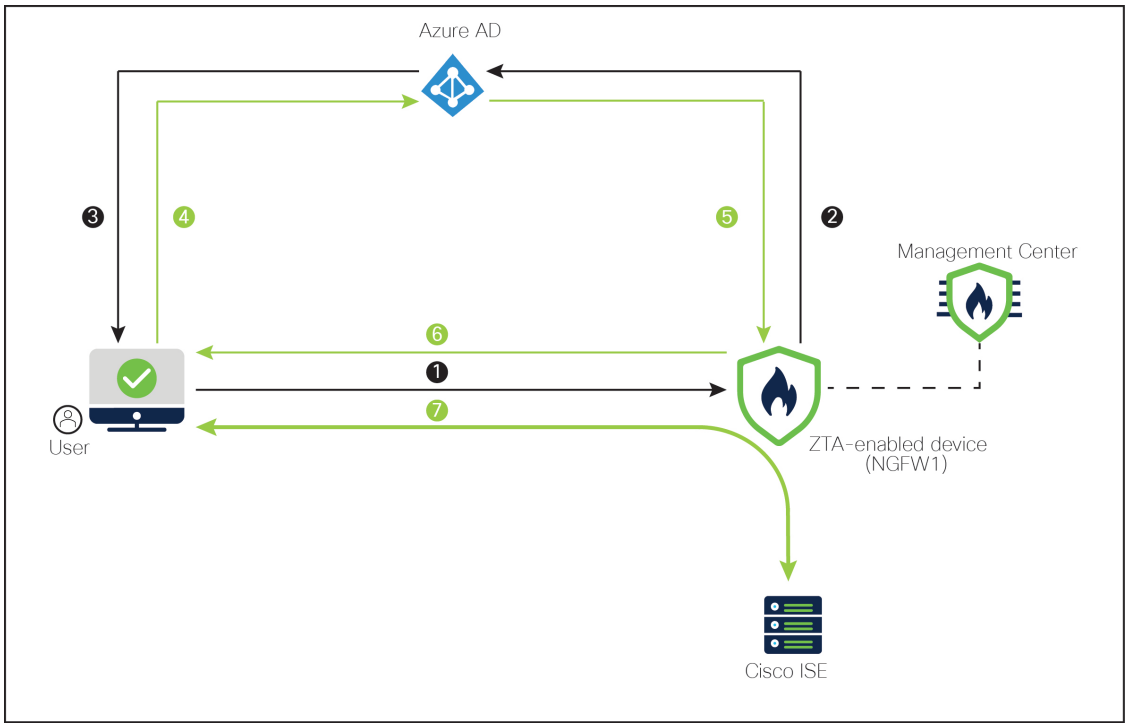
작업 인력이 네트워크에 완전히 액세스할 수 있게 되므로, 공격 표면이 증가하고 네트워크가 공격에 더 취약해집니다. 또한 직원들은 악성 콘텐츠가 포함되어 있을 가능성이 있는 파일을 포함하여 파일을 업로드할 수 있습니다.

Secure Firewall Management Center Zero Trust Access 정책은 애플리케이션을 어떻게 보호합니까?

네트워크 관리자가 방화벽에 대한 Zero Trust 액세스를 통합하면 모든 엔드포인트 디바이스에 소프트웨어를 설치하지 않고도 중요한 리소스 및 애플리케이션에 안전하게 원격 액세스할 수 있습니다. 이 기능은 성능을 향상시킬 뿐만 아니라 권한 부여를 단일 애플리케이션으로 제한하므로 잠재적인 공격 지점을 최소화합니다. 민감한 정보나 애플리케이션에 대한 액세스는 사용자 ID를 확인하고 요청의 상황을 확인하고 위험 분석을 수행한 후에만 부여됩니다. 또한 Zero Trust 애플리케이션 트래픽을 보호하기 위한 악성코드 및 파일 정책이 적용됩니다.

네트워크 토폴로지

다음 네트워크 토폴로지에는 데이터 센터에 설정된 threat defense 디바이스가 포함되어 있습니다. 디바이스의 아웃바운드 인터페이스에서 보안 영역이 설정됩니다.



위 그림에서 네트워크 관리자는 management center를 사용하여 **NGFW1**로 표시된 threat defense에 Zero Trust 정책을 구성하고 구축합니다. **Cisco ISE** 애플리케이션은 방화벽 뒤에 있는 데이터 센터에서 호스팅되며, 사용자는 Zero Trust 어플리케이션을 통해 방화벽에 액세스합니다. 참고: ISE는 AAA(Authentication, Authorization, and Accounting, 인증, 권한 부여 및 어카운팅)에는 사용되지 않습니다. Microsoft Azure Active Directory는 인증 및 권한 부여에 사용되는 SAML IdP 서버입니다. 네트워크 개체는 수신 요청의 공용 네트워크 소스 IP 주소를 회사 네트워크 내부의 라우팅 가능한 IP 주소로 변환하기 위해 생성됩니다.

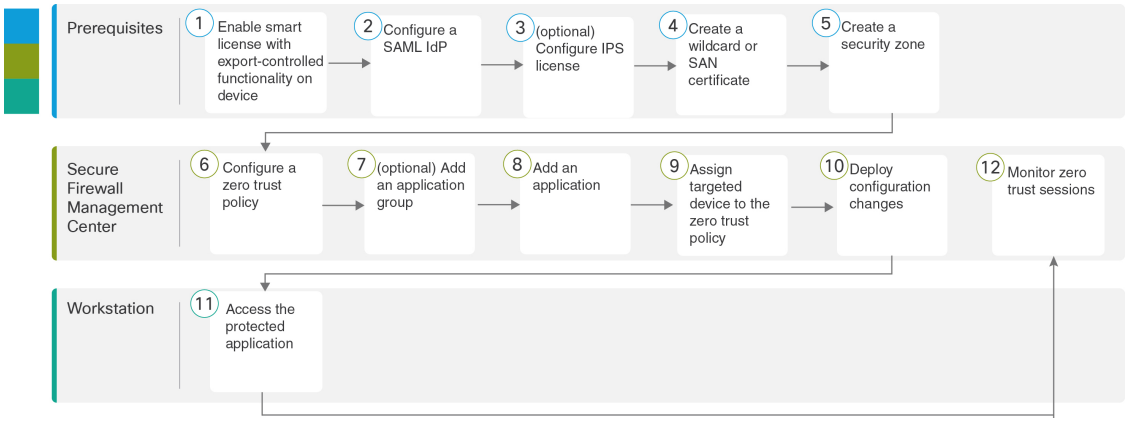
1. 사용자가 브라우저에 애플리케이션 URL을 입력합니다.
2. ZTA가 활성화된 관리 대상 디바이스는 사용자를 구성된 IdP로 안내합니다.
3. IdP에서 사용자에게 자격 증명을 입력하라는 메시지를 표시합니다.
4. 사용자 이름 및 비밀번호를 입력합니다.
5. IdP는 SAML 응답을 방화벽에 전송합니다. 사용자 ID 및 기타 필수 매개변수는 브라우저를 통해 SAML 응답에서 검색됩니다.
6. 검증에 성공하면 사용자가 애플리케이션으로 리디렉션됩니다.
7. 사용자에게 애플리케이션에 대한 액세스 권한이 허용됩니다. 선택적으로, 애플리케이션에 액세스하는 동안 위협 및 악성코드 방지가 적용됩니다.

Zero Trust Access 제한 사항

- 웹 애플리케이션(HTTPS)만 지원됩니다. 암호 해독 제외가 필요한 시나리오는 지원되지 않습니다.
- SAML IdP만 지원합니다.
- IPv6은 지원되지 않습니다. NAT66, NAT64 및 NAT46 시나리오는 지원되지 않습니다.
- 이 기능은 Snort 3이 활성화된 경우에만 Threat Defense에서 사용할 수 있습니다.
- 보호된 웹 애플리케이션의 모든 하이퍼링크에는 상대 경로가 있어야 하며, 개별 모드 클러스터에서 지원되지 않습니다.
- 가상 호스트에서 또는 내부 로드 밸런서 뒤에서 실행되는 보호된 웹 애플리케이션은 동일한 외부 및 내부 URL을 사용해야 합니다.
- 개별 모드 클러스터에서는 지원되지 않습니다.
- 엄격한 HTTP 호스트 헤더 검증이 활성화된 애플리케이션에서 지원되지 않습니다.
- 애플리케이션 서버가 여러 애플리케이션을 호스팅하고 TLS Client Hello의 SNI(Server Name Indication) 헤더를 기반으로 콘텐츠를 제공하는 경우, Zero Trust 애플리케이션 설정의 외부 URL은 해당 특정 애플리케이션의 SNI와 일치해야 합니다.

Zero Trust 애플레케이션 구성을 위한 End-to-End 절차

다음 순서도에서는 Secure Firewall Management Center에서 Zero Trust 액세스를 구성하는 워크플로우를 보여줍니다.



단계	설명
1	(사전 요건) Threat Defense에서 내보내기 제어 기능이 있는 스마트 라이선스를 활성화합니다.

단계	설명
2	(사전 요건) SAML IdP를 구성합니다.
3	(사전 요건) (선택 사항) IPS 라이선스를 구성합니다.
4	(사전 요건) 와일드카드 또는 SAN(Subject Alternative Name) 인증서를 생성합니다.
5	(사전 요건) 보안 영역을 생성합니다.
6	Zero Trust 애플리케이션 정책 생성
7	애플리케이션 그룹 생성.
8	애플리케이션 생성.
9	Zero Trust 액세스 정책에 대한 대상 디바이스 설정.
10	디바이스에 구성 구축.
11	보호된 애플리케이션 액세스.
12	Zero Trust 세션 모니터링.

Zero Trust 애플리케이션 정책 사전 요건

다음을 확인하십시오.

- 내보내기 제어 기능이 있는 스마트 라이선스 어카운트.
- 프라이빗 애플리케이션에 액세스하기 위한 인증 및 권한 부여용 IdP(SAML Identity Provider) 구성.
- 보안 제어 활성화를 위해 구성된 IPS 및 Threat 라이선스.
- 비공개 애플리케이션의 FQDN과 일치하는 와일드카드 또는 SAN(Subject Alternative Name, 주체 대체 이름) 인증서를 생성. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "인증서 등록 개체 추가" 섹션을 참조하십시오.

- management center에서 프라이빗 애플리케이션에 대한 액세스가 규제되는 보안 영역 생성. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "인터페이스 개요" 장에서 "보안 영역 및 인터페이스 그룹 개체 생성" 섹션을 참조하십시오.
- 공용 DNS 업데이트가 필요합니다.

인증서

다음 인증서를 생성해야 합니다.

- **Identity Certificate(ID** 인증서**)** - 이 인증서는 threat defense에서 애플리케이션으로 가장하는 데 사용됩니다. Threat Defense은 SAML SP(Service Provider, 서비스 제공자)로 동작합니다. 이 인증서는 프라이빗 애플리케이션의 FQDN에 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다.

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "인증서 등록 개체 추가" 섹션을 참조하십시오.

  이 예에서는 ID 인증서 **ZTAA-ID-Certificate**를 생성했습니다.

- **IdP** 인증서- IdP는 정의된 각 애플리케이션 또는 애플리케이션 그룹에 대한 인증서를 제공합니다. threat defense 에서 수신 SAML 어설션에서 IDP의 서명을 확인할 수 있도록 이 인증서를 구성해야 합니다.

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "인증서 등록 추가" 섹션을 참조하십시오.

  이 예시에서는 IdP 인증서 **Azure-AD-SAML-Certificate**를 생성합니다.

- **Application Certificate(**애플리케이션 인증서**)** - 사용자에서 애플리케이션으로의 암호화된 트래픽은 threat defense에서 이 인증서를 검사용으로 사용하여 암호 해독됩니다.

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "내부 인증서 개체 추가" 섹션을 참조하십시오.

  이 예에서는 애플리케이션 **ZTAA-ISE-GUI-Certificate**용 내부 인증서를 생성했습니다.

참고 IPS/악성코드 검사를 수행하지 않는 경우에도 연결 권한을 부여하기 위해 헤더의 쿠키를 확인하는 데 이 인증서가 필요합니다.

Zero Trust 애플리케이션 정책 생성

이 작업은 Zero Trust 애플리케이션 정책을 구성합니다.

시작하기 전에

다음을 확인하십시오.

- 애플리케이션에 액세스하는 threat defense 게이트웨이 인터페이스에서 확인할 도메인 이름.
- 비공개 애플리케이션에 대한 액세스를 규제하는 보안 영역. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "인터페이스 개요" 장에서 "보안 영역 및 인터페이스 그룹 개체 생성" 섹션을 참조하십시오.

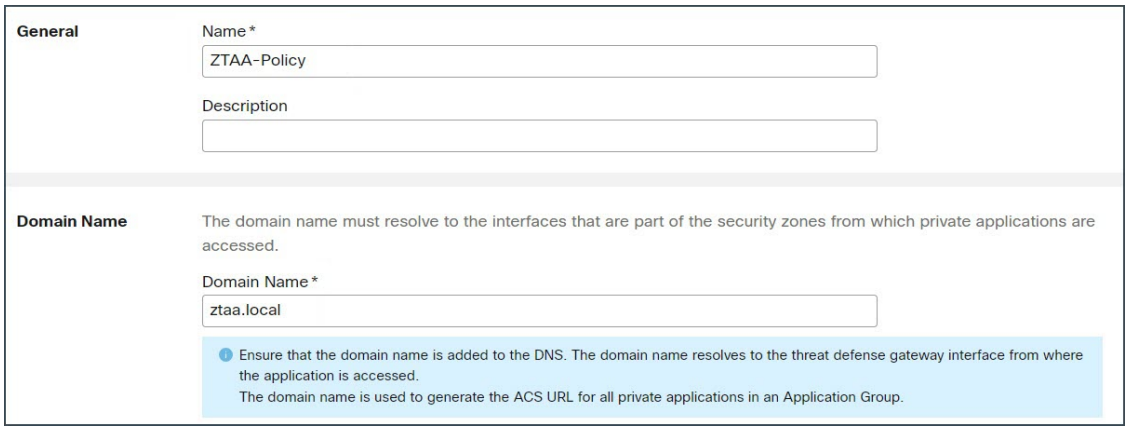
프로시저

단계 **1** management center에서, **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Zero Trust Application(Zero Trust** 어플리케이션**)**을 선택합니다.

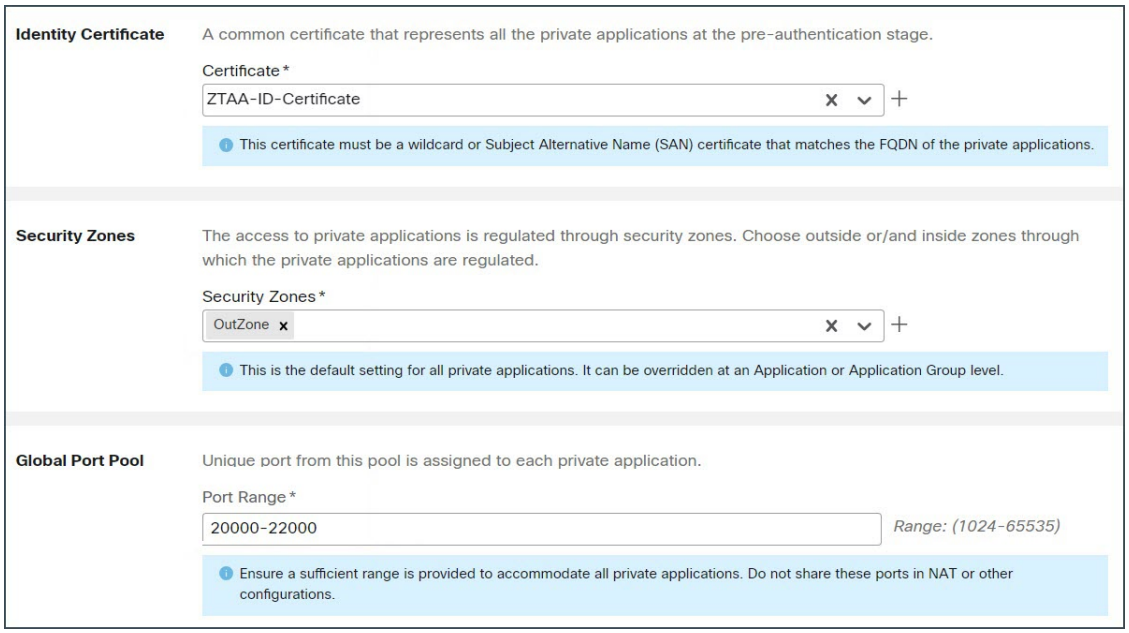
단계 **2** **Add Policy(**정책 추가**)**를 클릭합니다.

단계 **3** 아래에 설명된 대로 Zero Trust 정책 설정을 구성합니다.

- **Name(**이름**)**: 정책 이름을 입력합니다. 이 예시에서 Zero Trust 정책 이름은 **ZTAA-Policy**입니다.
- **Domain Name**(도메인 이름): 도메인 이름을 입력합니다. 이 도메인 이름은 애플리케이션 그룹의 모든 비공개 애플리케이션에 대한 ACS(Assertion Consumer Service, 어설션 소비자 서비스) URL을 생성하는 데 사용됩니다. 이 예에서 도메인 이름은 **ztaa.local**입니다.



- **IdP Certificate(IdP** 인증서**)**: 드롭다운 목록에서 기존 인증서를 선택합니다. 이 예에서는 생성된 ID 인증서 **ZTAA-ID-Certificate**를 선택합니다.
- **Security Zone(**보안 영역**)**: 드롭다운 목록에서 보안 영역을 선택합니다. 이 예에서는 보안 영역 **OutZone**을 생성했습니다.
- **Port Range(**포트 범위**)**: 이 풀의 고유한 포트가 각 프라이빗 애플리케이션에 할당됩니다. 이 포트 범위는 기존 NAT 범위와의 충돌을 방지합니다. 이 예에서는 기본값 **20000-22000**을 사용합니다.



단계 **4** **Security Controls(**보안 제어**)** 섹션에서 침입 또는 악성코드 및 파일 정책을 추가할 수 있습니다. 이러한 설정은 Zero Trust 애플리케이션 트래픽에 대한 침입 및 악성코드 방지 기능을 제공합니다.

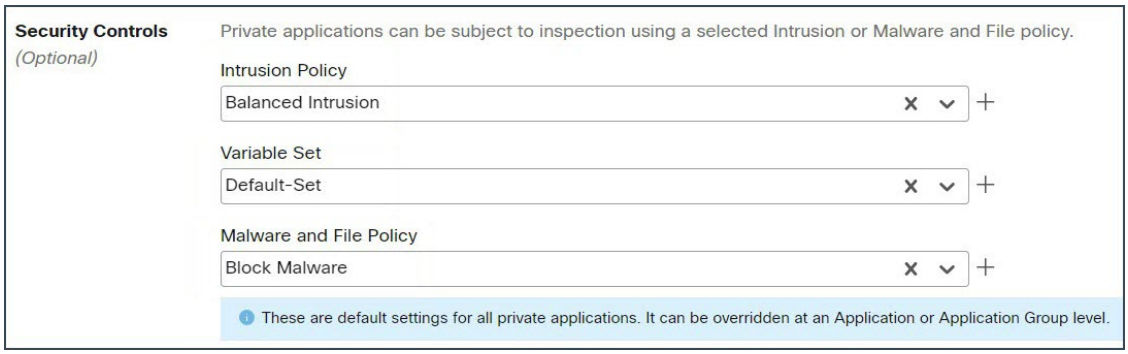
- **Intrusion Policy(**침입 정책**)** - 드롭다운 목록에서 기본 정책을 선택하거나 Add(추가) (+) 아이콘을 클릭하여 새 맞춤형 침입 정책을 생성합니다. 자세한 내용은 최신 버전의 Cisco Secure Firewall Management Center Snort 3 구성 가이드에서 사용자 지정 Snort 3 침입 정책 생성 주제를 참조하십시오. 이 예에서는 **Balanced Intrusion**이라는 침입 정책을 생성했습니다.

- **Variable Set(**변수 집합**)**: 드롭다운 목록에서 기본 변수 집합을 선택하거나 Add(추가) (+) 아이콘을 클릭하여 새 변수 집합을 생성합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "변수 집합 생성" 섹션을 참조하십시오. 이 예에서는 기본값 **Default-Set**를 사용했습니다.

- **Malware and File Policy(**악성코드 및 파일 정책**)**:

  드롭다운 목록에서 기존 정책을 선택하거나 Add(추가) (+) 아이콘을 클릭하여 새 맞춤형 악성코드 정책을 생성합니다.

  드롭다운 목록에서 기존 정책을 선택합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "네트워크 악성코드 보호 및 파일 정책" 장에서 "파일 정책 관리" 섹션을 참조하십시오. 이 예에서는 악성코드 정책 **Block Malware(**악성코드 차단**)**를 생성했습니다.



단계 **5** **Save(**저장**)**를 클릭합니다.

애플리케이션 그룹 생성

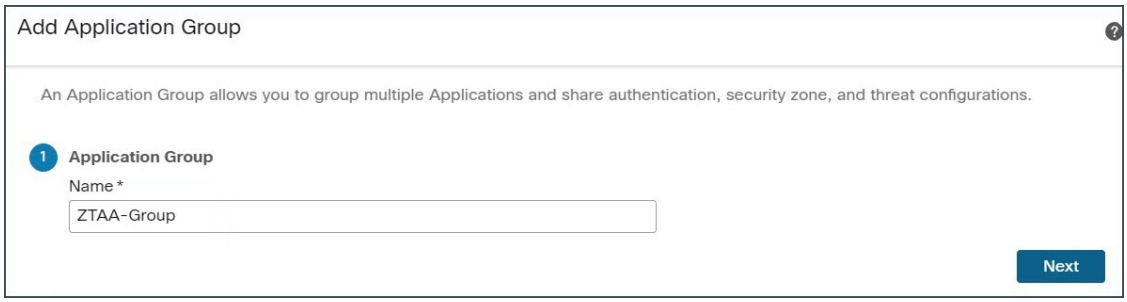
프로시저

단계 **1** management center에서, **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Zero Trust Application(Zero Trust** 어플리케이션**)**을 선택합니다.

단계 **2** Edit policy(정책 편집)를 클릭합니다.

단계 **3** **Add Application Group(**애플리케이션 그룹 추가**)**을 클릭합니다.

단계 **4** **Application Group(**애플리케이션 그룹**)** 섹션에서 **Name(**이름**)** 필드에 이름을 입력하고 **Next(**다음**)**를 클릭합니다. 이 예에서 애플리케이션 그룹 이름은 **ZTAA-Group**입니다.

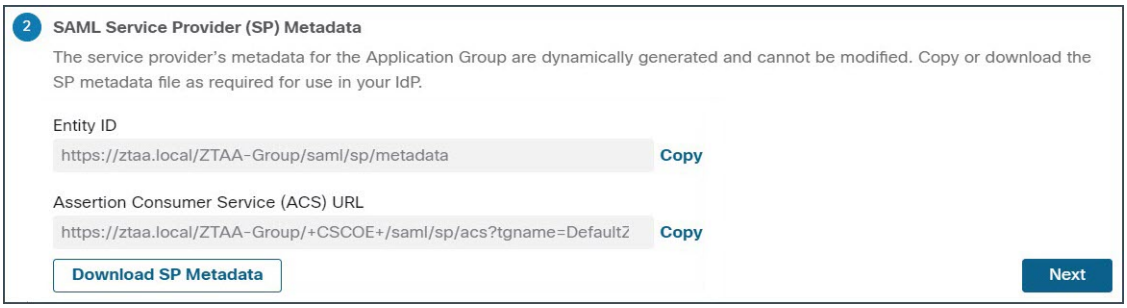


단계 **5** **SAML Service Provider (SP) Metadata(SAML** 서비스 제공자**(SP)** 메타데이터 섹션에서 이전 단계에서 제공한 구성 요소에서 데이터가 동적으로 생성됩니다.

- 애플리케이션 그룹: ZTAA-Group
- 도메인 이름: ztaa.local

Entity ID(엔터티 **ID)** 및 **ACS(Assertion Consumer Service) URL** 필드의 값을 복사하거나 **Download SP Metadata (SP** 메타데이터 다운로드**)**를 클릭하여 IdP에 추가할 수 있도록 이 데이터를 XML 형식으로 다운로드합니다.

이 예에서는 데이터가 XML 형식으로 다운로드되고 Azure Active Directory IdP에 업로드됩니다.



Next(다음**)**를 클릭합니다.

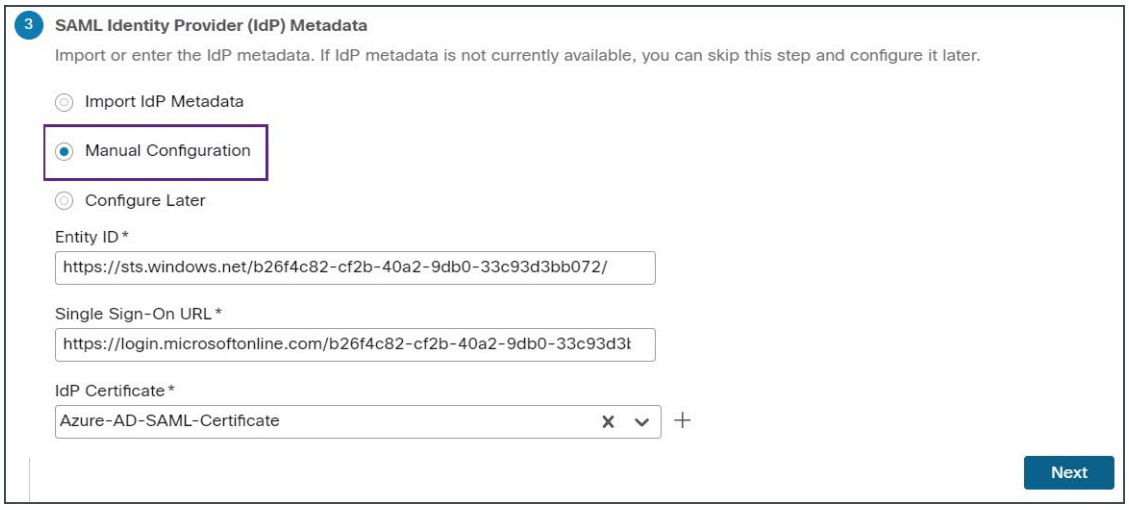
단계 **6** **SAML Identity Provider (IdP) Metadata(SAML ID** 제공자**(IdP)** 메타데이터**)** 섹션에서 메타데이터를 추가합니다.

이 예에서는 메타데이터를 수동으로 입력합니다.

메타데이터를 입력하려면 **Manual Configuration(**수동 구성**)**을 선택합니다.

- **Entity ID(**엔터티 **ID)**: SAML IdP에 정의된 URL을 입력하여 서비스 공급자를 고유하게 식별합니다. 이 예에서는 **https://sts.windows.net/ b26f4c82-cf2b-40a2-9db0-33c93d3bb072/** 를 사용합니다.
- **Single Sign-On URL(**단일 인증 **URL)**: SAML ID 공급자 서버에 로그인하기 위한 URL을 입력합니다. 이 예에서는 **https://login.microsoftonline.com/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/saml2** 를 사용합니다.
- **IdP Certificate(IdP** 인증서**)**: threat defense에 등록된 IdP의 인증서를 선택합니다.

  이 예에서는 생성된 IdP 인증서인 **Azure-AD-SAML-Certificate**를 선택합니다.



이 예에서는 수동 구성이 선택되어 있습니다.

Next(다음**)**를 클릭합니다.

단계 **7** **Re-authentication Interval** (재인증 간격) 섹션에서 **Timeout Interval** (시간 초과 간격) 필드에 값을 입력하고 **Next**(다음)를 클릭합니다. 재인증 간격을 사용하면 사용자가 다시 인증해야 하는 시기를 결정하는 값을 제공할 수 있습니다. 이 예에서는 기본값 **1440**을 사용합니다.

단계 **8** **Security Zones and Security Controls**(보안 영역 및 보안 제어)의 보안 영역 및 위협 설정은 상위에서 상속됩니다. 이 예에서는 기본값이 유지됩니다. **Next**(다음)를 클릭합니다.

단계 **9** 구성 요약을 검토합니다. 마침을 클릭합니다.

단계 **10** **Save**(저장)를 클릭합니다.

애플리케이션 그룹이 생성되고 Zero Trust Application(Zero Trust 애플리케이션) 페이지에 표시됩니다.

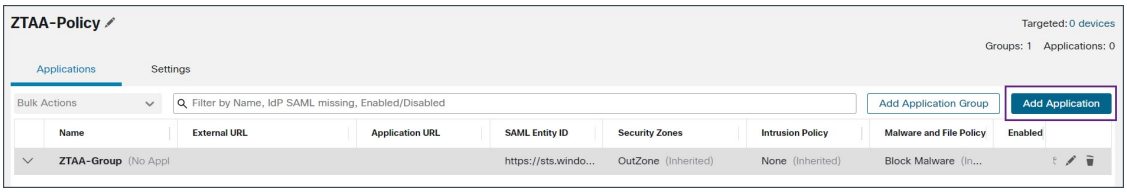
애플리케이션 생성

프로시저

단계 **1** **Policies**(정책) > **Access Control**(액세스 제어) > **Zero Trust Application**(**Zero Trust** 애플리케이션)을 선택합니다.

단계 **2** 정책을 선택합니다. 이 예에서는 **ZTAA-Policy**를 선택합니다.

단계 **3** **Add Application**(애플리케이션 추가)을 클릭합니다.



단계 **4** **Application Settings(**애플리케이션 설정**)** 섹션에서 다음 필드를 구성합니다.

- **Application Name(**애플리케이션 이름**)**: 애플리케이션 이름을 입력합니다. 이 예에서 애플리케이션 이름은 **ZTAA-ISE-GUI-Access**입니다.
- **External URL(**외부 **URL)**: 사용자가 애플리케이션에 액세스하는 데 사용하는 URL을 입력합니다. 이 예에서는 **https://ise-external.local**을 사용합니다.
- **Application URL(**애플리케이션 **URL)**: 기본적으로 외부 URL이 애플리케이션 URL로 사용됩니다. **Use External URL as Application URL(**외부 **URL**을 애플리케이션 **URL**로 사용**)** 체크 박스의 선택을 취소하여 다른 URL을 지정합니다. 이 예에서는 **https://ise.local**을 사용합니다.

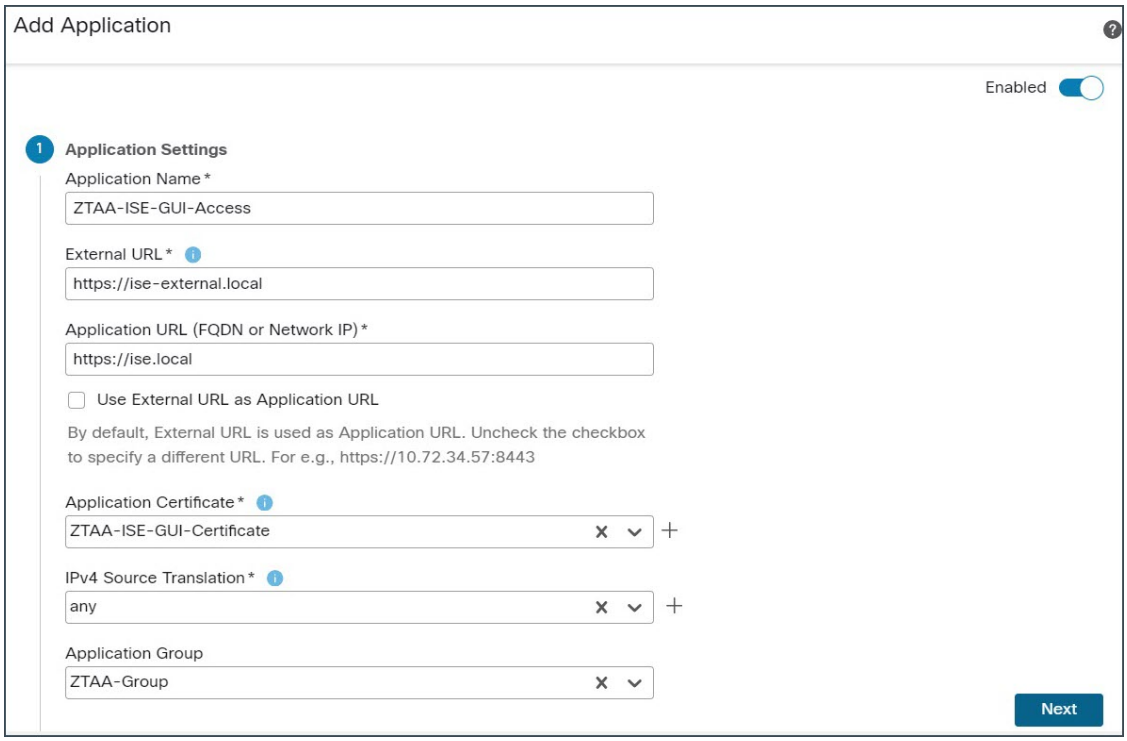
  Threat Defense에서 내부 DNS를 사용하는 경우, 애플리케이션을 확인하려면 애플리케이션 URL이 해당 DNS 내의 항목에 일치해야 합니다.
- **Application Certificate(**애플리케이션 인증서**)**: 프라이빗 애플리케이션용 인증서를 선택합니다.

  이 예에서는 생성된 내부 인증서 **ZTAA-ISE-GUI-Certificate**를 선택합니다.
- **IPv4 Source Translation(IPv4** 소스 변환**)**: 네트워크 개체 또는 개체 그룹은 수신 요청의 공용 네트워크 소스 IP 주소를 기업 네트워크 내부의 라우팅 가능한 IP 주소로 변환하는 데 사용됩니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "개체 관리" 장에서 "네트워크 개체 생성" 섹션을 참조하십시오.

  참고 Host 또는 Range 유형의 개체 또는 개체 그룹만 지원됩니다.
- **Application Group(**애플리케이션 그룹**)**: 드롭다운 목록에서 애플리케이션 그룹을 선택합니다. 애플리케이션 그룹 생성이 표시됩니다.

  참고 이 필드는 그룹 해제된 애플리케이션에 적용되지 않습니다.

이 예에서는 **ZTAA-Group** 애플리케이션 그룹을 사용합니다.



Next(다음**)**를 클릭합니다.

단계 **5** 구성 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

애플리케이션은 Zero Trust 애플리케이션 페이지에 나열되며 기본적으로 활성화됩니다.

참고 management center은 각 애플리케이션에 대한 진단 도구를 제공하여 Zero Trust 구성에서 발생할 수 있는 문제를 감지하여 문제 해결을 용이하게 합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드, X.Y의 "Zero Trust 액세스" 장에서 "Zero Trust 세션 모니터링" 섹션을 참조하십시오.

Zero Trust 액세스 정책에 대한 대상 디바이스 설정

각 Zero Trust 애플리케이션 정책은 여러 디바이스를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 정책을 구축할 수 있습니다.

프로시저

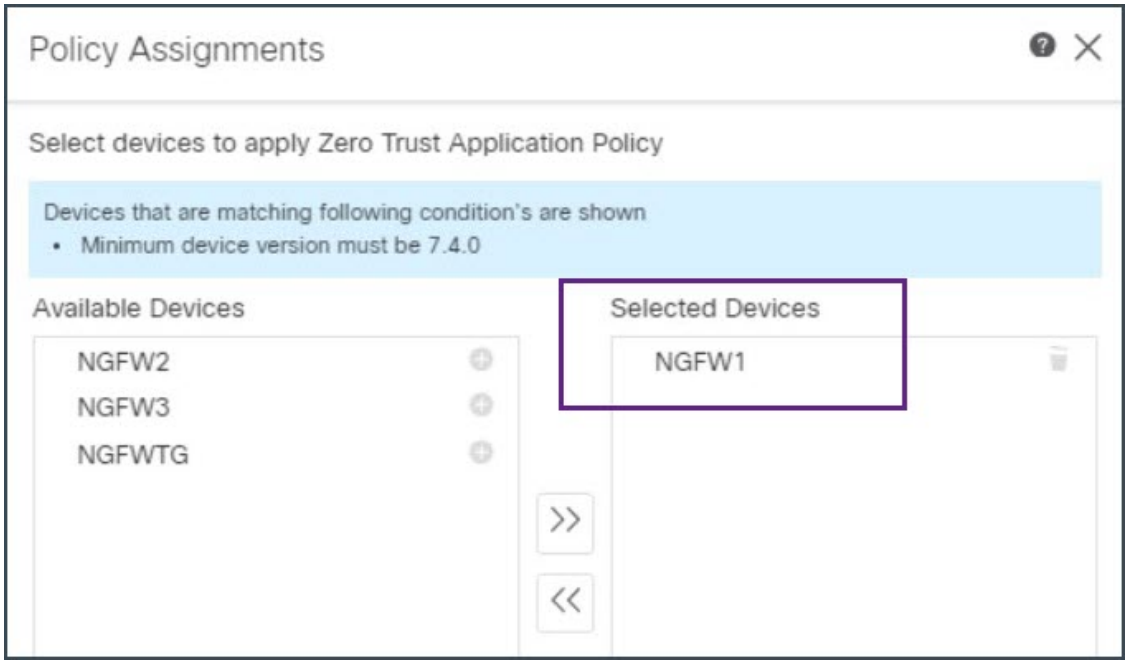
단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Zero Trust Application(Zero Trust** 애플리케이션**)**을 선택합니다.

단계 **2** 정책을 선택합니다. 이 예에서는 **ZTAA-Policy**를 선택합니다.

단계 **3** **Targeted Devices(**대상 디바이스**)**를 클릭합니다.

단계 **4** 구축하려는 디바이스를 선택합니다.

이 예에서는 **NGFW1**을 선택합니다.



단계 **5** **Apply(**적용**)**를 클릭하여 정책 할당을 저장합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

디바이스에 구성 구축

디바이스에 구성 구축

모든 구성을 완료한 후 매니지드 디바이스에 구축합니다.

프로시저

단계 **1** Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 그러면 구축 준비가 완료된 디바이스의 목록이 표시됩니다.

단계 **2** 구성 변경 사항을 구축할 디바이스 옆의 확인란을 선택합니다. 이 예에서 디바이스는 **NGFW1**입니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다. Deploy(구축) 대화 상자에서 구축이 Completed(완료)로 표시될 때까지 기다립니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 또는 **Validation Warnings(**검증 경고**)** 창에 이를 표시합니다. 전체 세부 정보를 보려면 **Validation Errors(**검증 오류**)** 또는 **Validation Warnings(**검증 경고**)** 링크를 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- **Proceed with Deploy(**구축 계속**)**: 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- **Close(**닫기**)**: 구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

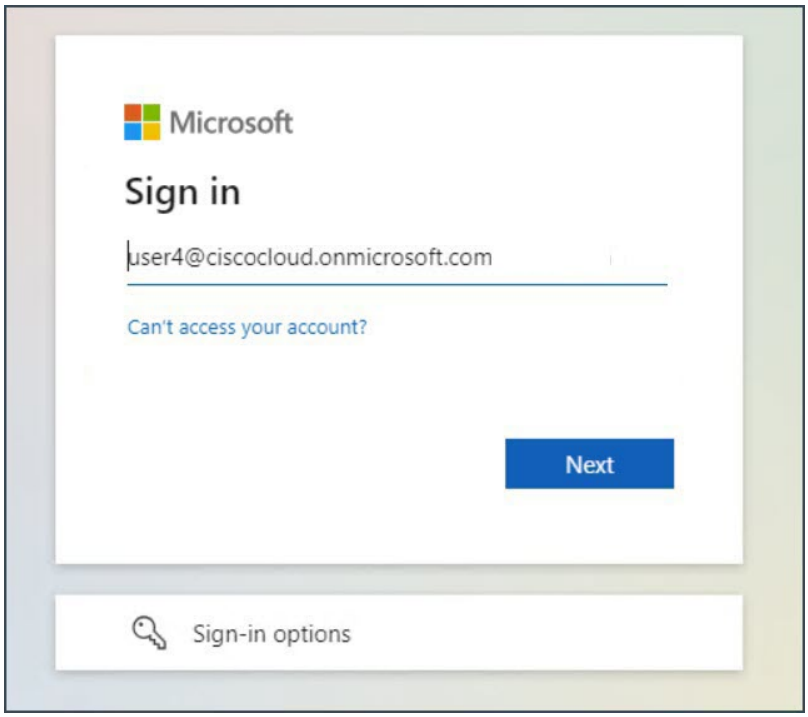
보호된 애플리케이션 액세스

구성 구축을 정상적으로 완료하고 나면 애플리케이션의 외부 URL을 사용하여 애플리케이션에 액세스할 수 있습니다.

프로시저

단계 **1** 클라이언트 컴퓨터에서 브라우저를 열고 외부 URL을 사용하여 보호된 애플리케이션에 액세스합니다. 이 예시에서 사용되는 외부 URL은 **https://ise-external.local**입니다.

사용자는 로그인 페이지로 리디렉션되고 SAML IdP에서 자격 증명을 입력하라는 메시지가 표시됩니다. 이 예에서 사용되는 SAML IdP는 Microsoft Azure Active Directory입니다.



단계 **2** 자격 증명을 제출한 후 IdP가 사용자를 인증하고 권한을 부여하고 응답의 SAML 어설션을 threat defense 디바이스로 전송하면 사용자는 애플리케이션으로 리디렉션됩니다.

단계 **3** 인증에 성공하면 사용자는 애플리케이션에 액세스할 수 있습니다. 이 예에서는 Cisco ISE 홈 페이지가 표시됩니다.

단계 **4** 사용자는 자신의 자격 증명을 사용하여 Cisco ISE에 로그인합니다.

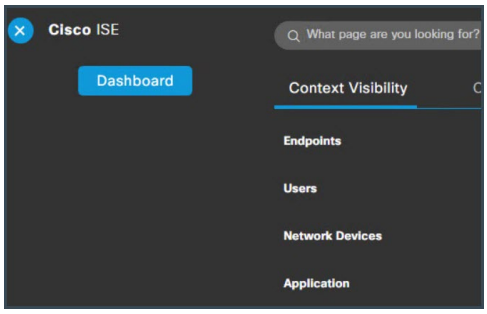
Zero Trust 애플리케이션 트래픽에 대한 악성코드 방지 테스트

사용자가 보호된 애플리케이션에 악성코드 파일을 업로드하려고 시도하면 ZTA 정책이 사용자 네트워크에서 악성코드 파일 업로드를 차단합니다.

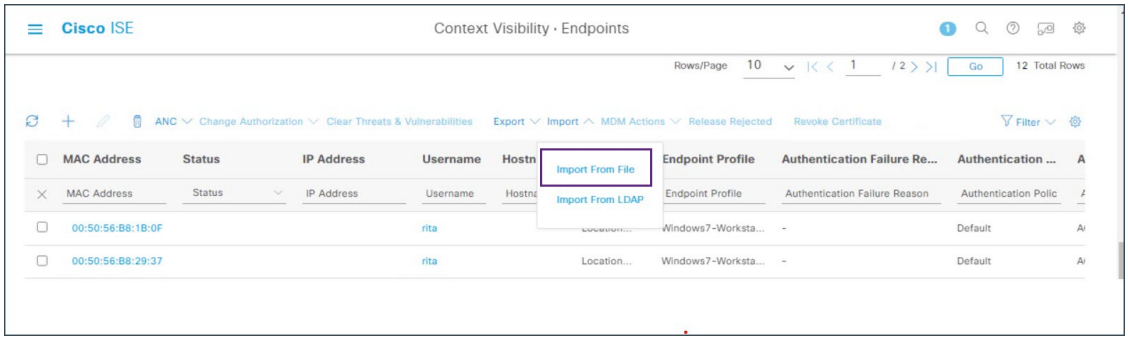
프로시저

단계 **1** Cisco ISE 애플리케이션에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**를 선택합니다.



단계 **3** 이 페이지를 아래로 스크롤하여 엔드포인트 목록을 찾은 다음 **Import(**가져오기**)** > **Import From File(**파일에서 가져오기**)**을 선택합니다.

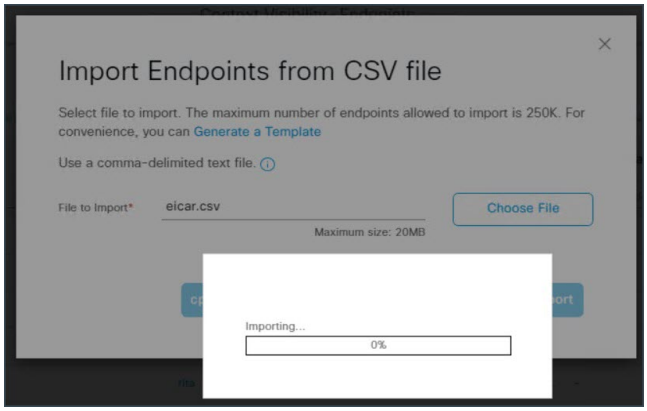


단계 **4** **Choose File(**파일 선택**)** 클릭하고 업로드할 백업 파일을 선택합니다. 파일을 선택하는 탐색 단계는 운영 체제에 따라 달라질 수 있습니다.

이 예에서는 사전 생성된 샘플 악성코드 파일을 선택합니다.

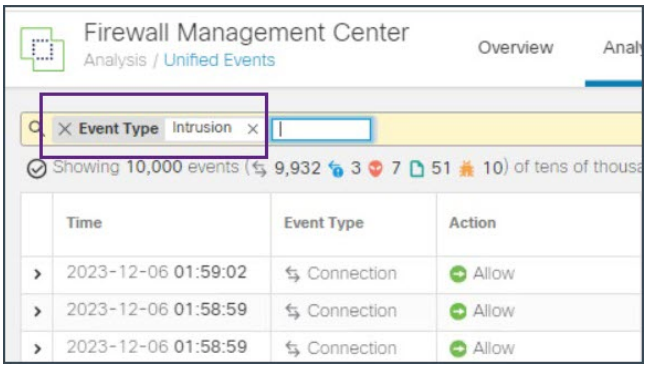
단계 **5** **Import(**가져오기**)**를 클릭합니다.

업로드 작업이 0% 이상 진행되지 않습니다. 이는 악성코드 파일이며, ZTA 정책에서 파일 업로드를 차단했습니다.



단계 **6** management center에 로그인하고 **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

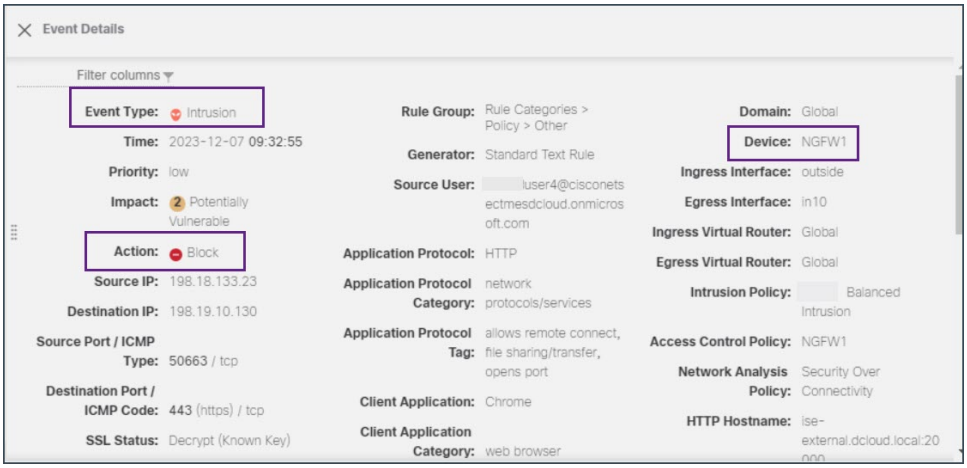
단계 **7** 검색 창에서 필터 **Event Type** (이벤트 유형)을 **Intrusion(**침입**)**으로 설정하고 **Apply(**적용**)**를 클릭합니다.



이 예에서는 슬라이딩 기본 시간을 **5**분으로 구성합니다. **Sliding Time Range(**슬라이딩 시간 범위**)**를 클릭합니다.

이벤팅 페이지는 악성 파일이 탐지 및 차단되었음을 표시합니다.

자세한 내용을 보려면 **Event Details(**이벤트 세부 사항**)** 페이지에서 이벤트를 더블 클릭하십시오.



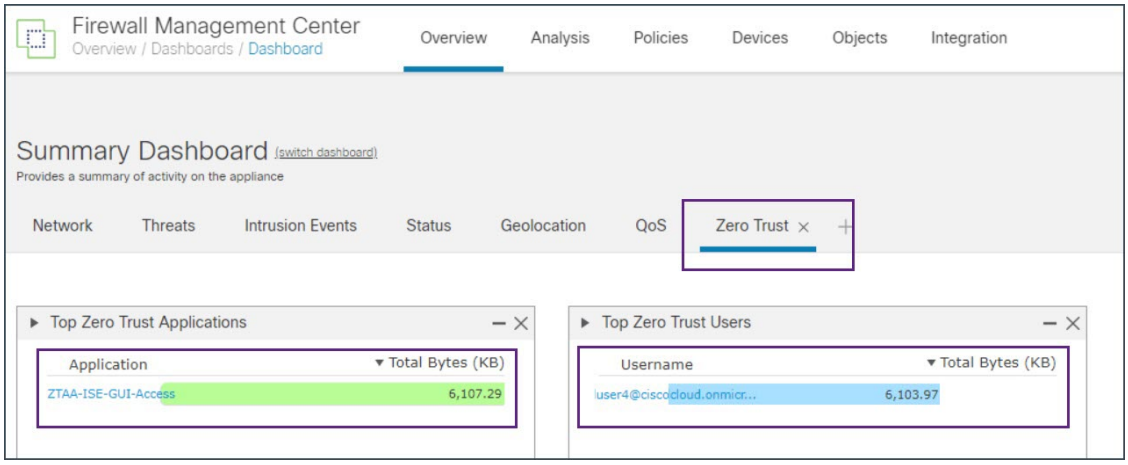
Zero Trust 세션 모니터링

Zero Trust 대시보드

Zero Trust 대시보드를 사용하면 디바이스의 활성 Zero Trust 세션에서 실시간 데이터를 모니터링할 수 있습니다. Zero Trust 대시보드에서는 management center에서 관리하는 상위 Zero Trust 애플리케이션 및 Zero Trust 사용자에 대한 요약을 제공합니다.

Overview(개요**)** > **Dashboards(**대시보드**)** > **Zero Trust(**제로 트러스트**)**를 선택하여 대시보드에 액세스합니다.

이 예에서 **Top Zero Trust Applications(**상위 **Zero Trust** 애플리케이션**)** 위젯은 Zero Trust 애플리케이션 **ZTAA_ISE_GUI_Access**와 애플리케이션에 액세스하는 사용자의 사용자 이름을 표시합니다.

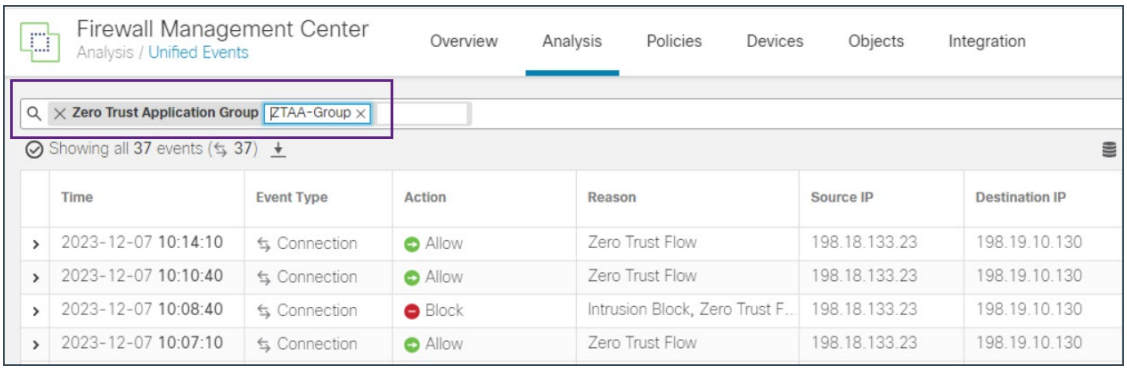


연결 이벤트

Zero Trust 세션을 설정한 후에는 해당 세션과 관련된 이벤트를 보고 사용자의 활동을 모니터링할 수 있습니다.

1. management center에서 **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.
2. 검색 창에서 **Zero Trust Application(Zero Trust** 애플리케이션**)**, **Zero Trust Application Group(Zero Trust** 애플리케이션 그룹**)** 또는 **Zero Trust Application Policy(Zero Trust** 애플리케이션 정책**)**를 검색하고 이를 생성하는 동안 지정한 해당 이름을 입력합니다.

   이 예에서는 **Zero Trust** 애플리케이션 그룹인 **ZTAA-Group**을 사용하여 이벤트를 검색합니다.



슬라이더를 오른쪽으로 스크롤하면 **Authentication Source(**인증 소스**)**, **Zero Trust Application(Zero Trust** 애플리케이션**)** 및 **Zero Trust Application Policy(Zero Trust** 애플리케이션 정책**)**를 볼 수 있습니다.