Zero Trust Access

다음 주제에서는 Zero Trust 애플리케이션 정책의 개요와 이러한 정책을 구성하고 구축하는 방법에 대한 개요를 제공합니다.

Zero Trust Access 정보

Zero Trust Access 기능은 ZTNA(제로 트러스트 네트워크 액세스) 원칙을 기반으로 합니다. ZTNA는 암시적 신뢰를 제거하는 제로 트러스트 보안 모델입니다. 이 모델은 사용자와 요청 컨텍스트를 확인한 뒤, 액세스 권한이 부여된 경우 위험을 분석한 후 최소 권한 액세스를 부여합니다.

Zero Trust Access를 사용하면 외부의 SAML IdP(Identity Provider) 정책을 사용하여 네트워크 내부(온프레미스) 또는 외부(원격)에서 보호된 웹 기반 리소스 및 애플리케이션에 대한 액세스를 인증하고 권한을 부여할 수 있습니다.

기능은 다음과 같습니다.

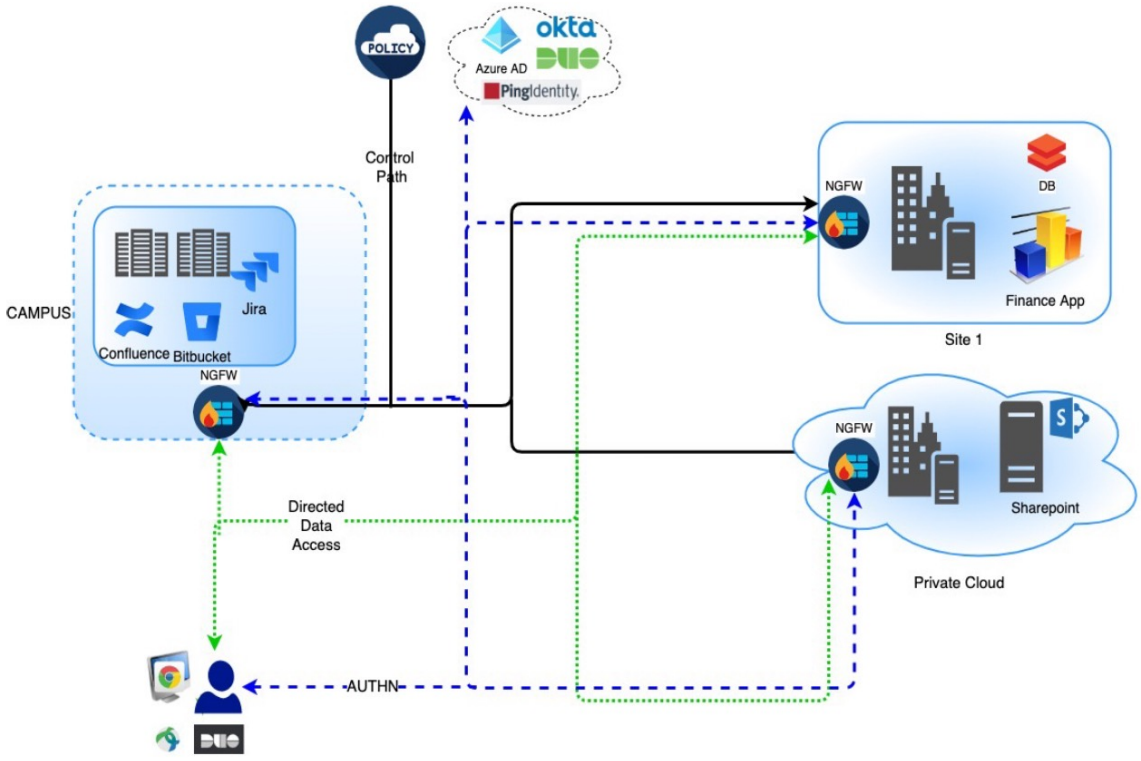
- Duo, Azure AD, Okta 및 기타 ID 제공자와 같은 여러 SAML 기반 ID 제공자를 지원합니다.

- Cisco Secure Client와 같은 클라이언트 애플리케이션은 보안 액세스를 위해 엔드포인트(클라이언트 디바이스)에 필요하지 않습니다.
- 액세스 및 인증은 브라우저를 통해 이루어집니다.
- 웹 애플리케이션(HTTPS)만 지원합니다.
- 클라이언트 디바이스 보안 상태는 Duo Health와 같은 에이전트를 통해 지원되며, 이를 사용하여 Duo의 정책에 대해 디바이스의 보안 상태를 평가하고 이를 기반으로 액세스를 제공할 수 있습니다. Okta 또는 PingID 같은 에이전트를 이용하여 보안 상태 평가를 지원하는 서드파티 ID 제공자와 함께 동일한 기능을 수행할 수 있습니다.
- HTTP-Redirect SAML 바인딩을 지원합니다.
- 애플리케이션 집합에서 Zero Trust 보호를 쉽게 활성화할 수 있는 애플리케이션 그룹을 지원합니다.
- Zero Trust 애플리케이션 트래픽에서 Threat Defense 침입 및 악성코드 방지를 활용합니다.

Secure Firewall Management Center 웹 인터페이스를 사용하여 프라이빗 애플리케이션을 정의하고 위협 정책을 할당할 수 있는 Zero Trust 애플리케이션 정책을 생성할 수 있습니다. 이 정책은 애플리케이션에 따라 관리자가 애플리케이션에 대한 위협 인식을 기반으로 검사 레벨을 결정합니다.

Zero Trust Access에서 Threat Defense가 작동하는 방법

그림 *1: Threat Defense* 구축



1. 원격 또는 온프레미스 사용자가 브라우저를 사용하여 엔드포인트에서 애플리케이션으로 연결하기 위한 HTTPS 요청을 보냅니다.
2. 애플리케이션을 보호하는 방화벽이 HTTPS 요청을 가로챕니다.
3. 방화벽은 인증을 위해 사용자를 애플리케이션에 구성된 IdP로 리디렉션합니다.

참고 그림에서 각 방화벽은 웹 애플리케이션 집합을 보호합니다. 사용자는 인증 및 권한 부여 후 방화벽 뒤에 있는 애플리케이션에 직접 액세스할 수 있습니다.

4. 인증 및 권한 부여 프로세스가 완료되면 방화벽에서 사용자의 애플리케이션 액세스를 허용합니다.

Zero Trust Access를 사용해야 하는 이유

Zero Trust Access는 애플리케이션 액세스에 대한 시행 지점으로 Threat Defense의 기존 구축을 활용합니다. 이를 통해 원격 및 온프레미스 사용자에 대한 애플리케이션별 권한 부여 및 애플리케이션별 터널을 통해 프라이빗 애플리케이션에 대한 세그먼트 액세스를 허용합니다.

이 기능을 사용하면 사용자에게 네트워크가 표시되지 않으며 사용자는 권한이 있는 애플리케이션에만 액세스할 수 있습니다. 네트워크의 한 애플리케이션에 대해 권한을 부여한다고 해서 네트워크의 다른 애플리케이션에 대해 묵시적 권한이 부여되는 것은 아니므로, 공격 표면이 크게 감소합니다. 즉, 애플리케이션에 대한 모든 액세스는 명시적으로 권한 부여되어야 합니다.

Threat Defense에 Zero Trust Access 기능을 추가하면 네트워크에 또 다른 디바이스를 설치하거나 관리하지 않고도 더 안전한 액세스 모델로 마이그레이션할 수 있습니다.

이 기능은 클라이언트가 필요하지 않고 애플리케이션 단위 액세스이므로, 관리하기 쉽습니다.

Zero Trust Access 구성의 구성 요소

새로운 구성은 Zero Trust 애플리케이션 정책, 애플리케이션 그룹 및 애플리케이션으로 구성됩니다.

- **Zero Trust** 애플리케이션 정책 - 애플리케이션 그룹과 그룹화되거나 그룹화되지 않은 애플리케이션으로 구성됩니다. 보안 영역 및 보안 제어 설정은 그룹 해제된 모든 애플리케이션 및 애플리케이션 그룹에 대해 전역 수준에서 연결됩니다.

  기본적으로 전역 포트 풀이 정책에 할당됩니다. 이 풀에서 구성된 각 프라이빗 애플리케이션에 고유한 포트가 자동으로 할당됩니다.

  Zero Trust 애플리케이션 정책은 애플리케이션 그룹과 그룹화되거나 그룹화되지 않은 애플리케이션으로 구성됩니다.

- 애플리케이션 그룹 - SAML 인증 설정을 공유하고 필요에 따라 보안 영역 및 보안 제어 설정을 공유할 수 있는 애플리케이션의 논리적 그룹으로 구성됩니다.

  애플리케이션 그룹은 전역 정책에서 보안 영역 및 보안 제어 설정을 상속하며 해당 값을 재정의할 수 있습니다.

  애플리케이션 그룹을 생성하면 동일한 SAML IdP 구성을 사용하여 여러 애플리케이션을 인증할 수 있습니다. 애플리케이션 그룹에 속한 애플리케이션은 애플리케이션 그룹의 SAML 구성을 상속합니다. 따라서 각 애플리케이션에 대해 SAML 설정을 구성할 필요가 없습니다. 애플리케이션 그룹이 생성된 후에는 IdP를 구성하지 않고도 새 애플리케이션을 추가할 수 있습니다.

  최종 사용자가 그룹에 속한 애플리케이션에 액세스하려고 할 때 사용자는 처음으로 애플리케이션 그룹에 인증됩니다. 사용자가 동일한 애플리케이션 그룹에 속한 다른 애플리케이션에 액세스하려고 하면 인증을 위해 IdP로 다시 리디렉션되지 않고 사용자에게 액세스 권한이 제공됩니다. 이렇게 하면 제한이 활성화된 경우 IdP가 애플리케이션 액세스 요청으로 오버로드되는 것을 방지하고 IdP 사용을 최적화합니다.

- 애플리케이션 - 두 가지 유형이 있습니다.

- 그룹 해제된 애플리케이션 - 독립형 애플리케이션입니다. 모든 애플리케이션에 대해 SAML 설정을 구성해야 합니다. 애플리케이션은 전역 정책에서 보안 영역 및 보안 제어 설정을 상속하며 애플리케이션에 의해 재정의될 수 있습니다.
- 그룹화된 애플리케이션 - 애플리케이션 그룹으로 그룹화된 여러 애플리케이션입니다. SAML 설정은 애플리케이션 그룹에서 상속되며 재정의할 수 없습니다. 그러나 각 애플리케이션의 보안 영역 및 보안 제어 설정은 재정의할 수 있습니다.

구성에는 다음 인증서가 필요합니다.

- **ID** 인증서 - 이 인증서는 threat defense에서 애플리케이션으로 가장하는 데 사용됩니다. Threat Defense는 SAML SP(서비스 제공자)로 작동합니다. 이 인증서는 프라이빗 애플리케이션의 FQDN에 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다. threat defense로 보호되는 모든 애플리케이션에 대한 공통 인증서입니다.
- **IdP** 인증서 - IdP는 정의된 각 애플리케이션 또는 애플리케이션 그룹에 대한 인증서를 제공합니다. threat defense에서 수신 SAML 어설션의 IDP 서명을 확인할 수 있도록 이 인증서를 구성해야 합니다.

참고 IdP 인증서는 일반적으로 메타데이터 파일 내에 포함됩니다. 그렇지 않을 경우 사용자는 애플리케이션 구성 중에 IdP 인증서를 즉시 사용할 수 있도록 해야 합니다.

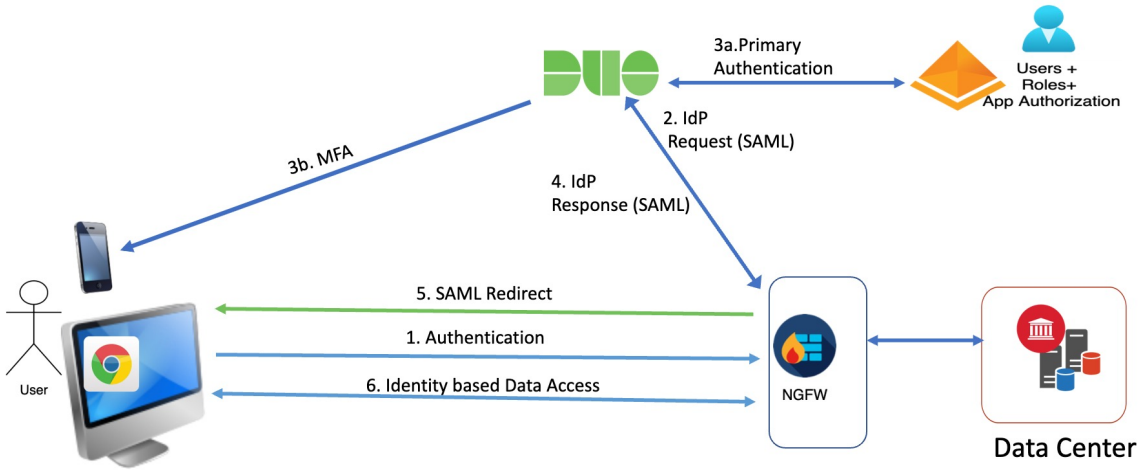
- 애플리케이션 인증서 - 사용자에서 애플리케이션으로의 암호화된 트래픽은 검사 목적으로 이 인증서를 사용하여 threat defense를 통해 암호를 해독합니다.

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

Zero Trust Access 워크플로우

이 그림은 Zero Trust Access 워크플로우를 보여줍니다.

그림 *2: Zero Trust Access* 워크플로우



워크플로우는 다음과 같습니다.

1. 사용자가 브라우저에 애플리케이션 URL을 입력합니다.
   - HTTPS 요청이 유효한 경우 사용자는 매핑된 포트로 리디렉션됩니다(6단계).
   - HTTPS 요청이 유효하지 않은 경우, 애플리케이션별 인증을 위해 사용자가 전송됩니다(2단계).
2. 사용자는 구성된 IdP(Identity Provider)로 리디렉션됩니다.
3. 1. 사용자는 구성된 기본 인증 소스로 리디렉션됩니다.
   2. 사용자에게 구성된 보조 다단계 인증(있는 경우)이 요구됩니다.
4. IdP는 SAML 응답을 Threat Defense에 전송합니다. 사용자 ID 및 기타 필수 매개변수는 브라우저를 통해 SAML 응답에서 검색됩니다.
5. 사용자는 애플리케이션으로 리디렉션됩니다.
6. 사용자는 검증에 성공해야 애플리케이션에 액세스할 수 있습니다.

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 3가 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 보호 중인 웹 애플리케이션은 동일한 외부 및 내부 URL을 사용해야 합니다.
- 개별 모드 클러스터에서는 지원되지 않습니다.
- 엄격한 HTTP 호스트 헤더 검증이 활성화된 애플리케이션에서는 지원되지 않습니다.
- 애플리케이션 서버가 여러 애플리케이션을 호스팅하고 TLS Client Hello의 SNI(Server Name Indication) 헤더를 기반으로 콘텐츠를 제공하는 경우, Zero Trust 애플리케이션 구성의 외부 URL은 해당 특정 애플리케이션의 SNI와 일치해야 합니다.

Zero Trust 애플리케이션 정책 사전 요건

사전 요건 유형	설명
라이선스	• 내보내기 제어 기능이 있는 스마트 라이선스 계정 • (선택 사항) IPS 및 위협 라이선스 - 보안 제어를 사용하는 경우 필요합니다.
컨피그레이션	프라이빗 애플리케이션의 FQDN과 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서를 생성합니다. 자세한 내용은 인증서 등록 개체 추가를 참고하십시오.
	프라이빗 애플리케이션에 대한 액세스가 규제되는 보안 영역을 만듭니다. 자세한 내용은 보안 영역 및 인터페이스 그룹 개체 생성를 참고하십시오.

Zero Trust 애플리케이션 정책 관리

Zero Trust 애플리케이션 정책을 생성, 편집 및 삭제할 수 있습니다.

프로시저

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

단계 **2** Zero Trust Acess 정책을 관리합니다.

- 생성 - **New Policy(**새 정책**)**를 클릭합니다. Zero Trust 애플리케이션 정책 생성, 8 페이지의 내용을 참조하십시오.
- 편집-**Edit(**수정**)** ( )를 클릭합니다. Zero Trust 애플리케이션 정책 편집, 14 페이지의 내용을 참조하십시오.
- 보고서 - **Report(**보고서**)** ( )를 클릭합니다.
- 삭제- **Delete(**삭제**)** ( )를 클릭합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Threat Defense에 구성을 구축하기 전에 경고가 없는지 확인합니다. 구성 변경 사항을 구축하려면 Cisco Secure Firewall Management Center 관리 가이드에서 구성 변경 구축을 참조하십시오.

Zero Trust 애플리케이션 정책 생성

이 작업은 Zero Trust 애플리케이션 정책을 구성합니다.

시작하기 전에

Zero Trust 애플리케이션 정책 사전 요건, 7 페이지에 나열된 모든 사전 요건을 완료합니다.

프로시저

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

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

단계 **3** **General(**일반**)** 섹션에서 **Name(**이름**)** 필드에 정책 이름을 입력합니다. Description(설명) 필드는 선택 사항입니다.

단계 **4** **Domain Name(**도메인 이름**)** 필드에 도메인 이름을 입력합니다.

도메인 이름이 DNS에 추가되었는지 확인합니다. 도메인 이름은 애플리케이션에 액세스하는 위협 방어 게이트웨이 인터페이스를 확인합니다. 도메인 이름은 애플리케이션 그룹의 모든 프라이빗 애플리케이션에 대한 ACS URL을 생성하는 데 사용됩니다.

단계 **5** **Identity Certificate(ID** 인증서**)** 드롭다운 목록에서 기존 인증서를 선택합니다.

인증서 등록 개체를 구성하려면 **Add(**추가**)** ( ) 아이콘을 클릭합니다. 자세한 내용은 인증서 등록 개체 추가를 참고하십시오.

단계 **6** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택합니다.

Add(추가**)** (+) 아이콘을 클릭하여 새 보안 영역을 추가합니다.

보안 영역을 추가하려면 보안 영역 및 인터페이스 그룹 개체 생성의 내용을 참조하십시오.

단계 **7** **Global Port Pool(**전역 포트 풀**)** 섹션에 기본 포트 범위가 표시됩니다. 필요한 경우 수정합니다. 포트 값 범위는 1024~65535입니다. 이 풀의 고유한 포트가 각 프라이빗 애플리케이션에 할당됩니다.

참고 이 포트 범위는 기존 NAT 범위와의 충돌을 방지합니다.

단계 **8** (선택 사항) **Security Controls(**보안 제어**)** 섹션에서 침입 또는 악성코드 및 파일 정책을 추가할 수 있습니다.

- **Intrusion Policy(**침입 정책**)** - 드롭다운 목록에서 기본 정책을 선택하거나 **Add(**추가**)** (+) 아이콘을 클릭하여 새 사용자 지정 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.
- **Variable Set(**변수 집합**)** - 드롭다운 목록에서 기본 변수 집합을 선택하거나 **Add(**추가**)** (+) 아이콘을 클릭하여 새 변수 집합을 생성합니다. 자세한 내용은 변수 집합 생성를 참고하십시오.

  참고 변수 집합을 사용하려면 매니지드 디바이스에 대한 Secure Firewall Threat Defense IPS 라이선스가 있어야 합니다.

- **Malware and File Policy(**악성코드 및 파일 정책**)** - 드롭다운 목록에서 기존 정책을 선택합니다. **Add(**추가**)** (+) 아이콘을 클릭하여 새로운 악성코드 및 파일 정책을 만듭니다. 자세한 내용은 파일 정책 관리를 참고하십시오.

단계 **9** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

1. 애플리케이션 그룹을 생성합니다. 애플리케이션 그룹 생성, 9 페이지의 내용을 참조하십시오.
2. 애플리케이션을 생성합니다. 애플리케이션 생성, 11 페이지의 내용을 참조하십시오.
3. Zero Trust 애플리케이션 정책을 디바이스와 연결합니다. Zero Trust Access 정책에 대한 대상 디바이스 설정, 13 페이지의 내용을 참조하십시오.
4. 컨피그레이션 변경사항을 구축합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 변경 사항 구축을 참조하십시오.

애플리케이션 그룹 생성

시작하기 전에

Zero Trust 애플리케이션 정책 생성, 8 페이지

프로시저

단계 **1** **Add Application Group(**애플리케이션 그룹 추가**)**을 클릭합니다.

단계 **2** **Application Group(**애플리케이션 그룹**)** 섹션에서 **Name(**이름**)** 필드에 이름을 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **3** **SAML Service Provider (SP) Metadata(SAML SP(**서비스 공급자**)** 메타데이터**)** 섹션에서 데이터는 동적으로 생성됩니다. **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. **Next(**다음**)**를 클릭합니다.

단계 **4** **SAML Identity Provider (IdP) Metadata(SAML IdP(ID** 제공자**)** 메타데이터**)** 섹션에서 다음 방법 중 하나를 사용하여 메타데이터를 추가합니다.

- **XML File Upload(XML** 파일 업로드**)** - 파일을 선택하거나 XML 파일을 끌어다 놓습니다.

  Entity ID(엔터티 **ID)**, **Single Sign-On URL(**단일 인증**)**, **IdP Certificate(IdP** 인증서**)**의 세부 정보가 표시됩니다.

- **Manual Configuration(**수동 구성**)** - 다음 단계를 수행합니다.
  - **Entity ID(**엔터티 **ID)** - SAML IdP에 정의된 URL을 입력하여 서비스 공급자를 고유하게 식별합니다.
  - **Single Sign-On URL(**단일 인증 **URL)** - SAML ID 공급자 서버에 로그인하기 위한 URL을 입력합니다.
  - **IdP Certificate(IdP** 인증서**)** - Threat Defense에 등록된 IdP의 인증서를 선택하여 IdP가 서명한 메시지를 확인합니다.

    새 인증서 등록 개체를 구성하려면 **Add(**추가**)** (+) 아이콘을 클릭합니다. 자세한 내용은 인증서 등록 추가을 참조하십시오.

- **Configure Later(**나중에 구성**)** - IdP 메타데이터가 없는 경우 나중에 구성할 수 있습니다.

Next(다음**)**를 클릭합니다.

단계 **5** **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.

단계 **6** **Security Zones and Security Controls(**보안 영역 및 보안 제어**)** 섹션에서 보안 영역 및 위협 설정은 상위 정책에서 상속됩니다. 이러한 설정을 재정의할 수 있습니다. **Next(**다음**)**를 클릭합니다.

단계 **7** 구성 요약을 검토합니다. **Edit(**편집**)**을 클릭하여 섹션의 세부 정보를 수정합니다. 마침을 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

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

다음에 수행할 작업

1. 애플리케이션 생성, 11 페이지.
2. 컨피그레이션 변경사항을 구축합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 변경 사항 구축을 참조하십시오.

애플리케이션 생성

그룹화 또는 그룹 해제된 애플리케이션을 생성하려면 이 작업을 사용합니다.

시작하기 전에

1. Zero Trust 애플리케이션 정책 생성, 8 페이지.
2. 애플리케이션 그룹 생성, 9 페이지(그룹 애플리케이션의 경우에만 필요).

프로시저

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

단계 **2** 정책을 선택합니다.

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

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

- **Application Name(**애플리케이션 이름**)** - 애플리케이션 이름을 입력합니다.
- **External URL(**외부 **URL)** - 사용자가 애플리케이션에 액세스하는 데 사용하는 URL을 입력합니다.
- **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.

  Threat Defense에서 내부 DNS를 사용하는 경우, 애플리케이션을 확인하려면 애플리케이션 URL이 해당 DNS 내의 항목에 일치해야 합니다.
- **Application Certificate(**애플리케이션 인증서**)** - 프라이빗 애플리케이션용 인증서를 선택합니다. 내부 인증서 개체를 구성하려면 **Add(**추가**)** (+) 아이콘을 클릭합니다. 자세한 내용은 내부 인증서 개체 추가를 참고하십시오.
- **IPv4 Source Translation(IPv4** 소스 변환**)**- 드롭다운 목록에서 NAT에 대한 소스 네트워크를 선택합니다. 네트워크 개체를 생성하려면 **Add(**추가**)** (+) 아이콘을 클릭합니다. 자세한 내용은 네트워크를 참고하십시오.

이 네트워크 개체 또는 개체 그룹은 수신 요청의 퍼블릭 네트워크 소스 IP 주소를 기업 네트워크 내의 라우팅 가능한 IP 주소로 변환하는 데 사용됩니다.

참고 호스트 또는 범위 유형의 개체 또는 개체 그룹만 지원됩니다.

- **Application Group(**애플리케이션 그룹**)** - 드롭다운 목록에서 애플리케이션 그룹을 선택합니다. 애플리케이션 그룹 생성, 9 페이지의 내용을 참조하십시오.

참고 이 필드는 그룹 해제된 애플리케이션에 적용되지 않습니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** 애플리케이션 유형에 따라 다릅니다.

- 그룹화된 애플리케이션의 경우 **SAML Service Provider (SP) Metadata(SAML SP(**서비스 공급자**)** 메타데이터**)**, **SAML Identity Provider (IdP) Metadata(SAML IdP(ID** 제공자**)** 메타데이터**)**, **Re-authentication Interval(**재인증 간격**)**은 애플리케이션 그룹에서 상속되며 사용자가 구성할 필요가 없습니다.
- 그룹 해제된 애플리케이션의 경우 다음 단계를 수행합니다.
  1. **SAML Service Provider (SP) Metadata(SAML SP(**통신 사업자**)** 메타데이터**)** 섹션에서 데이터는 동적으로 생성됩니다. IdP의 엔터티 **ID** 또는 **ACS(Assertion Consumer Service) URL**을 복사하거나 **Download SP Metadata(SP** 메타데이터 다운로드**)**를 클릭하여 IdP에 추가할 수 있도록 이 데이터를 XML 형식으로 다운로드합니다. **Next(**다음**)**를 클릭합니다.
  2. **SAML Identity Provider (IdP) Metadata(SAML IdP(ID** 제공자**)** 메타데이터**)** 섹션에서 다음 방법 중 하나를 사용하여 메타데이터를 추가합니다.
     - **XML File Upload(XML** 파일 업로드**)** - 파일을 선택하거나 XML 파일을 끌어다 놓습니다.

       Entity ID(엔터티 **ID)**, **Single Sign-On URL(**단일 인증**)**, **IdP Certificate(IdP** 인증서**)**의 세부 정보가 표시됩니다.
     - **Manual Configuration(**수동 구성**)** - 다음 단계를 수행합니다.
       - **Entity ID(**엔터티 **ID)** - SAML IdP에 정의된 URL을 입력하여 서비스 공급자를 고유하게 식별합니다.
       - **Single Sign-On URL(**단일 인증 **URL)** - SAML ID 공급자 서버에 로그인하기 위한 URL을 입력합니다.
       - **IdP Certificate(IdP** 인증서**)** - Threat Defense에 등록된 IdP의 인증서를 선택하여 IdP가 서명한 메시지를 확인합니다.

         새 인증서 등록 개체를 구성하려면 **Add(**추가**)** (+) 아이콘을 클릭합니다. 자세한 내용은 인증서 등록 추가을 참조하십시오.
     - **Configure Later(**나중에 구성**)** - IdP 메타데이터가 없는 경우 나중에 구성할 수 있습니다.

  Next(다음**)**를 클릭합니다.

3. **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.

단계 **7** **Security Zones and Security Controls(**보안 영역 및 보안 제어**)** 섹션에서 보안 영역 및 위협 설정은 상위 정책 또는 애플리케이션 그룹에서 상속됩니다. 이러한 설정을 재정의할 수 있습니다. **Next(**다음**)**를 클릭합니다.

단계 **8** 구성 요약을 검토합니다. **Edit(**편집**)**을 클릭하여 섹션의 세부 정보를 수정합니다. 마침을 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

애플리케이션은 Zero Trust Application(Zero Trust 애플리케이션) 페이지에 나열되며 기본적으로 활성화됩니다.

다음에 수행할 작업

1. Zero Trust Access 정책에 대한 대상 디바이스 설정, 13 페이지.
2. 컨피그레이션 변경사항을 구축합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 변경 사항 구축을 참조하십시오.

Zero Trust Access 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.

시작하기 전에

1. Zero Trust 애플리케이션 정책 생성, 8 페이지.
2. 애플리케이션 그룹 생성, 9 페이지.
3. 애플리케이션 생성, 11 페이지.

프로시저

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

단계 **2** 정책을 선택합니다.

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

단계 **4** 다음 방법 중 하나를 사용하여 정책을 구축하려는 디바이스를 선택합니다.

- **Available Devices(**사용 가능한 디바이스**)** 목록에서 디바이스를 선택하고 >> 또는 **Add(**추가**)** ( ) 아이콘을 클릭합니다.
- **Selected Devices(**선택한 디바이스**)** 목록에서 디바이스를 제거하려면 디바이스를 선택하고 << 또는 **Delete(**삭제**)** ( ) 아이콘을 클릭합니다.

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

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 변경 사항 구축을 참조하십시오.

Zero Trust 애플리케이션 정책 편집

Zero Trust 애플리케이션 정책, 애플리케이션 그룹 또는 애플리케이션의 설정을 편집할 수 있습니다.

프로시저

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

단계 **2** 편집할 Zero Trust 애플리케이션 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** Zero Trust 애플리케이션 정책을 편집합니다.

다음 설정을 변경하거나 다음 작업을 수행할 수 있습니다.

- Name and Description(이름 및 설명) - 정책 이름 옆에 있는 **Edit(**수정**)** ( )을 클릭하고 원하는 대로 변경한 다음 **Apply(**적용**)**를 클릭합니다.
- 정책 설정을 수정하려면 다음을 수행합니다.
  - **Settings(**설정**)**를 클릭합니다.
  - 필요에 따라 설정을 수정합니다.

    중요 SAML ACS URL의 도메인 이름을 편집하면 애플리케이션 액세스가 중단됩니다.

  - **Save(**저장**)**를 클릭합니다.
- 애플리케이션 그룹 설정을 수정하려면 다음을 수행합니다.
  - **Applications(**애플리케이션**)**를 클릭합니다.

- 편집할 애플리케이션 그룹 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.
- 각 섹션에서 **Edit(**편집**)**을 클릭하여 필요에 따라 설정을 수정합니다.

  중요 애플리케이션 그룹 이름을 편집하면 애플리케이션 액세스가 중단됩니다.

- 섹션에서 설정을 수정한 후 **Apply(**적용**)**를 클릭합니다.
- **Finish(**마침**)**를 클릭합니다.
- **Save(**저장**)**를 클릭합니다.

- 애플리케이션 설정을 수정하려면 다음을 수행합니다.
  - **Applications(**애플리케이션**)**를 클릭합니다.
  - 편집할 애플리케이션 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.
  - 각 섹션에서 **Edit(**편집**)**을 클릭하여 필요에 따라 설정을 수정합니다.

    중요 애플리케이션 이름을 편집하면 애플리케이션 액세스가 중단됩니다.

  - 섹션에서 설정을 수정한 후 **Apply(**적용**)**를 클릭합니다.
  - **Finish(**마침**)**를 클릭합니다.
  - **Save(**저장**)**를 클릭합니다.
- 여러 애플리케이션을 활성화, 비활성화 또는 삭제하려면 애플리케이션을 선택하고 필요한 대량 작업을 클릭한 다음 **Save(**저장**)**를 클릭합니다.

  참고 이러한 작업은 마우스 오른쪽 버튼 클릭 메뉴에서도 수행할 수 있습니다.

  - 모든 애플리케이션을 활성화하려면 **Bulk Actions(**대량 작업**)** > **Enable(**활성화**)**을 클릭합니다.
  - 모든 애플리케이션을 비활성화하려면 **Bulk Actions(**대량 작업**)** > **Disable(**비활성화**)**을 클릭합니다.
  - 모든 애플리케이션을 삭제하려면 **Bulk Actions(**대량 작업**)** > **Delete(**삭제**)**를 클릭합니다.
- **Return to Zero Trust Application(Zero Trust** 애플리케이션으로 돌아가기**)**을 클릭하여 정책 페이지로 돌아갑니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. Cisco Secure Firewall Management Center 관리 가이드의 구성 변경 사항 구축을 참조하십시오.

Zero Trust 세션 모니터링

연결 이벤트

Zero Trust 애플리케이션 정책을 구축하고 나면 새 필드를 사용할 수 있습니다. 테이블 보기에 필드를 추가하려면 다음을 수행합니다.

1. **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 선택합니다.
2. **Table View of Connection Events(**연결 이벤트 테이블 보기**)** 탭으로 이동합니다.
3. 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 표시되는 필드를 변경하려면 임의의 열 이름에서 **x** 아이콘을 클릭하여 필드 선택기를 표시합니다.
4. 다음 필드를 선택합니다.
   - 인증 소스
   - 제로 트러스트 애플리케이션
   - 제로 트러스트 애플리케이션 그룹
   - 제로 트러스트 애플리케이션 정책
5. **Apply(**적용**)**를 클릭합니다.

연결 이벤트에 대한 자세한 내용은 Secure Firewall Management Center 관리 가이드의 연결 및 보안 관련 연결 이벤트를 참조하십시오.

Zero Trust 대시보드

Zero Trust 대시보드를 사용하면 디바이스의 활성 Zero Trust 세션에서 실시간 데이터를 모니터링할 수 있습니다.

Zero Trust 대시보드는 Management Center에서 관리하는 상위 Zero Trust 애플리케이션 및 Zero Trust 사용자에 대한 요약을 제공합니다. **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Zero Trust**를 선택하여 대시보드에 액세스합니다.

대시보드에는 다음과 같은 위젯이 있습니다.

- 상위 Zero Trust 애플리케이션
- 상위 Zero Trust 사용자

CLI 명령

디바이스 CLI에 로그인하고 다음 명령을 사용합니다.

CLI 명령	설명
show running-config zero-trust	Zero Trust 구성에 대해 실행 중인 구성을 보려는 경우
show zero-trust	런타임 Zero Trust 통계 및 세션 정보를 표시하려는 경우
show cluster zero-trust	클러스터의 노드 전체에서 Zero Trust 통계의 요약을 표시하려는 경우
clear zero-trust	Zero Trust 세션 및 통계를 지우려는 경우
show counters protocol zero_trust	Zero Trust 플로우의 적중 횟수를 보려는 경우

진단 도구

진단 도구는 Zero Trust 구성으로 발생 가능한 문제를 탐지하여 문제 해결 프로세스를 지원합니다. 진단은 다음 2가지 유형으로 분류할 수 있습니다.

- 애플리케이션별 진단은 다음과 같은 문제를 탐지하는 데 사용됩니다.
  - DNS 관련 문제
  - 소켓이 열리지 않는 등의 잘못된 구성, 분류 및 NAT 규칙 관련 문제
  - Zero Trust 정책 또는 SSL 규칙 구축 문제
  - 소스 NAT 문제 및 PAT 풀 소진 문제
- 일반 진단은 다음과 같은 문제를 탐지하는 데 사용됩니다.
  - 강력한 암호 라이선스가 활성화되지 않음
  - 잘못된 애플리케이션 인증서
  - SAML 관련 문제
  - 홈 에이전트 및 클러스터 대량 동기화 문제

진단 도구를 실행하려면 다음을 수행합니다.

1. 문제를 해결하려는 Zero Trust 애플리케이션 옆에 있는 진단( )을 클릭합니다. **Diagnostics(**진단**)** 대화 상자가 표시됩니다.
2. **Select Device(**디바이스 선택**)** 드롭다운 목록에서 디바이스를 선택하고 **Run(**실행**)**을 클릭합니다. 진단 프로세스가 완료되면 **Reports(**보고서**)** 탭에서 보고서가 생성됩니다.
3. 로그를 보거나 복사하거나 다운로드하려면 **Logs(**로그**)** 탭을 클릭합니다.

Zero Trust 액세스 기록

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Zero Trust 액세스 개선 사항	7.4.1	7.4.1	• 이제 애플리케이션에 대한 NAT의 소스 네트워크를 구성할 수 있습니다. 구성된 네트워크 개체 또는 개체 그룹은 수신 요청의 퍼블릭 네트워크 소스 IP 주소를 애플리케이션 네트워크 내의 라우팅 가능한 IP 주소로 변환하는 데 사용됩니다. • 이제 문제 해결 프로세스를 촉진하는 진단 도구를 사용할 수 있습니다. 이 도구는 Zero Trust 구성에서 발생할 수 있는 문제를 감지합니다.
Zero Trust Access	7.4.0	7.4.0	사용자의 개인 디바이스에 추가 소프트웨어가 없어도 사용자가 프라이빗 애플리케이션에 액세스할 수 있습니다. 이 기능은 SAML 기반 인증을 활용하며 Duo는 물론 다른 모든 주요 ID 제공자를 지원합니다.