보안 방화벽에서 제로 트러스트 원격 액세스 구축 구성

목차
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>배경 정보</u>
<u>네트워크 다이어그램</u>
<u>필수 구성</u>
<u>일반 컨피그레이션</u>
<u>애플리케이션 그룹 구성</u>
<u>애플리케이션 그룹 1: 듀오를 IdP로 사용</u>
<u>응용 프로그램 그룹 2: Microsoft Enterprise ID(Azure AD)를 IdP로 사용</u>
<u>애플리케이션 구성</u>
<u>응용 프로그램 1: FMC 웹 UI 테스트(응용 프로그램 그룹 1의 멤버)</u>
<u>애플리케이션 2: CTB 웹 UI(애플리케이션 그룹 2의 멤버)</u>
<u>다음을 확인합니다.</u>
<u>모니터링</u>
<u>문제 해결</u>
관련 정보

소개

이 문서에서는 보안 방화벽에서 클라이언트리스 제로 트러스트 액세스 원격 액세스 구축을 구성하 는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- FMC(Firepower Management Center)
- 기본 ZTNA 지식
- SAML(Basic Security Assertion Markup Language) 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Firewall 버전 7.4.1
- FMC(firepower Management Center) 버전 7.4.1
- Duo as IdP(Identity Provider)
- Microsoft Entra ID(이전, Azure AD)를 IdP로 사용

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

제로 트러스트 액세스 기능은 ZTNA(Zero Trust Network Access) 원칙을 기반으로 합니다. ZTNA는 암시적 신뢰를 없애는 제로 트러스트 보안 모델입니다. 모델은 사용자, 요청의 컨텍스트, 액세스 권 한이 부여된 경우 위험을 분석한 후 최소 권한 액세스 권한을 부여합니다.

ZTNA의 현재 요구 사항 및 제한 사항은 다음과 같습니다.

- FMC 버전 7.4.0에서 관리되는 Secure Firewall 버전 7.4.0에서 지원됨(Firepower 4K Series)
- FMC 버전 7.4.1에서 관리되는 Secure Firewall 버전 7.4.1에서 지원됨(다른 모든 플랫폼)
- 웹 애플리케이션(HTTPS)만 지원됩니다. 암호 해독 제외가 필요한 시나리오는 지원되지 않습니다.
- SAML IdP만 지원합니다.
- 원격 액세스를 위해서는 공용 DNS 업데이트가 필요합니다.
- IPv6는 지원되지 않습니다. NAT66, NAT64 및 NAT46 시나리오는 지원되지 않습니다.
- 이 기능은 Snort 3이 활성화된 경우에만 위협 방어에서 사용할 수 있습니다.
- 보호된 웹 응용 프로그램의 모든 하이퍼링크에는 상대 경로가 있어야 합니다.
- 가상 호스트에서 실행되거나 내부 로드 밸런서 뒤에서 실행되는 보호된 웹 애플리케이션은 동 일한 외부 및 내부 URL을 사용해야 합니다.
- 개별 모드 클러스터에서는 지원되지 않습니다.
- 엄격한 HTTP 호스트 헤더 검증이 활성화된 응용 프로그램에서는 지원되지 않습니다.
- 애플리케이션 서버가 여러 애플리케이션을 호스팅하고 TLS Client Hello의 SNI(Server Name Indication) 헤더를 기반으로 콘텐츠를 제공하는 경우, 제로 트러스트 애플리케이션 컨피그레 이션의 외부 URL이 해당 특정 애플리케이션의 SNI와 일치해야 합니다.
- 라우팅 모드에서만 지원됨
- Smart License 필요(평가 모드에서 작동하지 않음)

보안 방화벽의 Zero Trust Access에 대한 자세한 내용 및 내용은 <u>Cisco Secure Firewall</u> <u>Management Center Device Configuration Guide, 7.4를</u> 참조하십시오.

구성

이 문서에서는 ZTNA의 원격 액세스 구축을 중점적으로 다룹니다.

이 예제 시나리오에서는 원격 사용자가 보안 방화벽 뒤에서 호스팅되는 테스트 FMC 및 Cisco CTB(Telemetry Broker)의 웹 사용자 인터페이스(UI)에 액세스해야 합니다. 다음 다이어그램에 나와 있는 것처럼, 두 개의 서로 다른 IdP, 즉 Duo와 Microsoft Entra ID를 통해 이러한 애플리케이션에 액 세스할 수 있습니다.

네트워크 다이어그램



토폴로지 다이어그램

- 1. 원격 사용자는 Secure Firewall 뒤에서 호스팅되는 애플리케이션에 액세스해야 합니다.
- 2. 각 애플리케이션에는 공용 DNS 서버에 DNS 항목이 있어야 합니다.
- 3. 이러한 애플리케이션 이름은 Secure Firewall Outside 인터페이스의 IP 주소로 확인해야 합니다.
- 4. 보안 방화벽은 애플리케이션의 실제 IP 주소를 확인하고 SAML 인증을 사용하여 각 애플리케 이션에 대해 각 사용자를 인증합니다.

필수 구성

IdP(Identity Provider) 및 DNS(Domain Name Server)

- 응용 프로그램 또는 응용 프로그램 그룹은 Duo, Okta 또는 Azure AD와 같은 SAML IdP(Identity Provider)에서 구성해야 합니다. 이 예에서는 Duo 및 Microsoft Entra ID가 IdP로 사용됩니다.
- IdPs에서 생성된 인증서 및 메타데이터는 보안 방화벽에서 애플리케이션을 구성할 때 사용됩

니다

내부 및 외부 DNS 서버

- 외부 DNS 서버(원격 사용자가 사용)에는 애플리케이션의 FQDN 항목이 있어야 하며 보안 방 화벽 외부 인터페이스 IP 주소로 확인해야 합니다
- 내부 DNS 서버(보안 방화벽에서 사용)에는 애플리케이션의 FQDN 항목이 있어야 하며 애플 리케이션의 실제 IP 주소로 확인되어야 합니다

인증서

다음 인증서는 ZTNA 정책 컨피그레이션에 필요합니다.

- ID/프록시 인증서: 보안 방화벽에서 애플리케이션을 가장하는 데 사용됩니다. 여기서 Secure Firewall은 SAML SP(Service Provider)의 역할을 합니다. 이 인증서는 프라이빗 애플리케이션 의 FQDN과 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다(인증 전 단계 의 모든 프라이빗 애플리케이션을 나타내는 공통 인증서).
- IdP 인증서: 인증에 사용되는 IdP는 정의된 각 애플리케이션 또는 애플리케이션 그룹에 대한 인증서를 제공합니다. 이 인증서는 보안 방화벽이 수신 SAML 어설션에 대한 IdP 서명을 확인할 수 있음(애플리케이션 그룹에 대해 정의된 경우 전체 애플리케이션 그룹에 대해 동일한 인증서가 사용됨)
- 애플리케이션 인증서: 원격 사용자로부터 애플리케이션으로 전송되는 암호화된 트래픽은 보 안 방화벽에 의해 해독되어야 합니다. 따라서 각 애플리케이션의 인증서 체인과 개인 키를 보 안 방화벽에 추가해야 합니다.

일반 컨피그레이션

새 Zero Trust 애플리케이션을 구성하려면 다음 단계를 수행합니다.

- 1. Policies(정책) > Access Control(액세스 제어) > Zero Trust Application(제로 트러스트 애플리 케이션)으로 이동하고 Add Policy(정책 추가)를 클릭합니다.
- 2. 필수 필드를 완료합니다.

a) 일반: 정책의 이름 및 설명을 입력합니다.

b) 도메인 이름: DNS에 추가된 이름이며 애플리케이션이 액세스되는 위협 방어 게이트웨이 인 터페이스로 확인되어야 합니다.

✤ 참고: 도메인 이름은 애플리케이션 그룹의 모든 개인 애플리케이션에 대한 ACS URL을 생성 하는 데 사용됩니다.

c) ID 인증서: 이 인증서는 인증 전 단계의 모든 개인 애플리케이션을 나타내는 공통 인증서입니 다. ✤ 참고: 이 인증서는 전용 애플리케이션의 FQDN과 일치하는 와일드카드 또는 SAN(주체 대체 이름) 인증서여야 합니다.

d) 보안 영역: 사설 애플리케이션이 규제되는 외부 또는/및 내부 영역을 선택합니다.

e) 전역 포트 풀: 이 풀의 고유 포트가 각 개인 애플리케이션에 할당됩니다.

f) 보안 제어(선택 사항): 프라이빗 애플리케이션이 검사 대상인지 여부를 선택합니다.

이 샘플 컨피그레이션에서는 다음 정보를 입력했습니다.

	 Presente de Terre Terret des factories 				
<pre>base base base base base base base base</pre>	*> Return to Zero Trust Application Add a Zero	Trust Application Po	licy	Cancel Save	
Served Served Served Served res S	Zero Trust Applica	tion Policy protects private app	fications with identity based access, intrusion protection, and malware and file inspection.		
Series III Image:		IdP			
Under the finite In the finite Derivation In the finite In the finite interference in the structure to the structure part of the security grows from the high phase applications are In the finite interference interferenc		Connect	Namet		
Image: Image		Grenteral	ZTNA-TAC		
Second 2 Second 2 <td< th=""><th></th><th></th><th>Description</th><th></th><th></th></td<>			Description		
Sevent Name The density have and the store that the the first less that use goal of the security zeros from which private applications are applications are stored to goal of the security zeros from which private applications are stored to goal of the security zeros. The security zeros from which private applications are stored to goal of the security zeros. The security zeros from which private applications are stored to goal of the security zeros. The security zeros from which private applications are stored to goal of the security zeros. The security zeros. Security Zeros The security applications are stored to goal of the security zeros. Decise which are stored to store to from which private applications are stored to goal of the security zeros. Decise which are stored to store to from which private applications are stored to f					
Benalt Name To downstructures takets to be structures to the str					
Security Zears According to public the problem and public the proble		Domain Name	The domain name must resolve to the interfaces that are part of the security zones from which private applications are		
Image: Section Control Image: Section			accessed.		
Image: Control in the second control into the DOD. The docet interpret rescale the rescale target particular is the application of the control. Image: Control interpret rescale the docet interpre			Southan Marrie		
Security Corrections Notice spectrate the subject to length and applications at the give-applications at the give-application			© Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where		
Security Certification Control certification Cartification Cartificatio			the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.		
Meeting Cardination A contract certification that represents all the private applications to the private applications to the private applications. Cardination The certification target and the certification target applications to republication. Secority Corest: The certification target applications to republication. Cardination target applications to republication. The certification target applications. Secority Corest: The certification target applications. Cardination target applications. The certification target applications. Secority Corest: The certification target applications. The certification target applications. The certification target applications. The certification target applications. The certification target applications. The certification target target applications. The certification certification target applications. The certification certification target target applications. The certification certification target target applications. The certification certification certification target target applications. The certification certificatio					
Security junction The control private any private approximation is the private approximation is the private approximation is the private approximation. Private and Private and Private approximation is the private approximation is the private approximation. Security Zones The control private approximation is the private approximation in the private approximation. Security Zones The control private approximation is the private approximation. Security Zones The control private approximation. Security Zones The trans the stand set the private approximation. Security Zones The trans the stand set the private approximation. Security Zones The trans the stand set the private approximation. Security Zones The private approximation. Security Zones The private approximation. Security Controls The trans attraction the poil is assigned to each private application. Private application. Private applications. Security Controls The stand set the stand set the private applications. Security Controls The stand set the stand set the stand set the private applications. Security Controls The stand set the sta		Identify Cartificate	A common coefficials that represents all the polyate applications at the pre-surthentication stress		
ZitMu-Viblicand-cert x In the sections must be available of Subject Admundte have (SAU) certificate that must be the FORM of the private applications. Security Zenes: The access to private applications are regulated: Singling Term x In this the distant section for all points applications. Private applications are regulated: Singling Term In this the distant section for all points applications. Private applications are regulated: Singling Term In this the distant section for all points applications. Private applications are regulated: Singling Term In this the distant section for a points applications. Private applications are regulated: Singling Term In this point is assigned to each private applications. Private applications are regulated: In this point is assigned to the point applications. Private applications are regulated: In this point is applications are regulated: Singling Term In this point is applications are regulated: In this point is point applications are regulated intrusion or Malause and File policy. Materia Materia Materia In this point file Policy Materia Materia In this point file Policy Materia In this point file Policy		identity Certificate	Certificate*		
In texticute true to a validate of a fuldate a fundate a bindite and fundate to the QDM of the private application. Security Zones: Descrity Z			ZTNA-Widcard-cert × v +		
Security Zones The access to sphilate applications are regulated. Security Zones Consist ** Outside ** ** Outside ** * The is the adult string for all pluste applications. * Port Renge* * Doctoreations. * Outside regulated the schedule adpluste applications. * Port Renge* * Doctoreations. * Port Renge* * Doctoreations. * Port and applications can be subject to happection using a selected intrusion or Malaure and File policy. Malace and File Policy * None * Malace and file Policy * Outside adult file Policy * N			This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.		
Security Zones The access to private applications is regulated. Image: The access to private applications is regulated. The access to private applications are regulated. Image: The access to private applications. The access to private applications. Image: The access to private applications. The access to private application. Image: The access to private applications. Private applications. Image: The access to private application. Private applications. Image: The access to private application and to private application. Private applications and private applications. Image: The access to private application and to private application. Private applications and private applications. Image: The access to private application and the application and private applications. Private applications and private applications. Image: The access to private application and the application and private a					
which the private applications are regulated. Security Zones* On his the default setting for all private applications. It can be overhiden at an Application Group twet. Global Pert Peet Unique pert from this pool is assigned to each private application. Pert Barrye* 20000-2000 20000-2000 Reging: (1024-65553) Of Ensure a sufficient range is private application. Do not have these ports in NAT or other Construction Reging: Controls (Optional) Private applications can be subject to inspection using a selected Intrusion or Malware and File policy. Note Note		Security Zones	The access to private applications is regulated through security zones. Choose outside or/and inside zones through		
Security Controls Private applications can be subject to inspection using a selected intrusion or Mailware and File policy. Security Controls Private applications can be subject to inspection using a selected intrusion or Mailware and File policy. Window File Policy Private applications can be subject to inspection using a selected intrusion or Mailware and File policy. Window File Policy None Window File Policy None Window File Policy None None + None + Mailware and File Policy + None + <th></th> <th></th> <th>which the private applications are regulated.</th> <th></th> <th></th>			which the private applications are regulated.		
Internation Internation			Security Zones*		
It is the default stering for all provide applications. It is a bedreated or of Application Of Applicatio Of Application Of Application Of Application Of Application Of A			A V		
Global Pert Pert Unique port from this pool is assigned to each private application. Port Range* 2000-2000 Renge: (1024-65539) © Brane applications can be subject to inspection using a selected intrusion or Malware and File policy. Renge: (1024-65539) Security Controls (Optional) Phote applications can be subject to inspection using a selected intrusion or Malware and File policy. Kingsiene X Y More X Y Malware and File Policy Y Y More Y Y Malware and File policy Y Y			This is the default setting for all private applications. It can be overridden at an Application or Application Group level.		
Global Per Ped Unique port (music happed) Is assigned to each private application. Per 2000-22000 Range: (1/024-65533) © Enum a sufficient range is provided to accommodate at private applications. Do not share these ports in NAT or other configurations. Security Controls ((Optional)) Phote applications can be subject to inspection using a selected intrusion or Mahware and File policy. Variable Set None None + Makeare and File Policy + None + Makeare and File policy. * None + Makeare and File policy. * None * None * None * None *					
Security Centrest (Optional) Phote applications can be subject to inspection using a selected intrusion or Malware and File policy. Note: Phote applications Watabase and File Policy + Maker and File Policy - Maker		Global Port Pool	Unique port from this pool is assigned to each private application.		
Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate and private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate and private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate and private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is provided to accommodate and private applications. Do not share these ports in NAT or other endparations. Ensure a sufficient range is private applications. Do not share these ports in NAT or other			2000-2200 Range: (1024-65535)		
Security Centrals Photos applications can be subject to inspection using a selected intrusion or Malwase and File policy. (Optional) Photos applications Variable Set			Foruse a sufficient range is pensided to accommodate all reliance applications. To not share these ports is NAT or other		
Security Centres Physice applications can be subject to inspection using a selected intrusion or Malware and File policy. (Optional) Intrusion Policy None > Valiable Set Mone > Mone > Descent of File policy. Mone > Mone > Policy + Mone > Policy +			configurations.		
Security Controls Philate applications can be subject to inspection using a selected intrusion or Malware and File policy. (Optional) Intrusion Policy Mone					
(Optional) Hetrusian Paley Note: X · · · + Values Set Note: · · · · · · Note: · · · · · · Note: · · · · · · · Note: · · · · · · ·		Security Controls	Private applications can be subject to inspection using a selected intrusion or Malware and File policy.		
None × + Variable Set None Makeare and File Policy + Mone × Others are defail and the policy and policities. It is to execute the target and the policities are benefitied and the benefities are benefities are benefities and the benefities are benefities and the benefities are benefiti		(Optional)	Intrusion Policy		
Variable Set None + Mahware and File Policy None * * * * * * * * * * * * * * * * * *			None × v +		
None Image: Control of the Policy None Image: Control of the Policy Image: Control of the Policy Image: Control of the Policy			Variable Set		
Makeware and Tile Policy + + None + + Description of the policy activity activity activity to a policy activity of the policy			NUM V T		
			None X V +		
THE TABLE ARE ADDRESS TO ADDRESS			Trans are defuil artitize for all minute analizations. It can be manifolded at an Analization or Analyzation former local		

이 경우에 사용되는 ID/프록시 인증서는 사설 애플리케이션의 FQDN과 일치시키기 위한 와일드카 드 인증서입니다.

Firewall Managem Devices / Certificates	ent Center	Overview Analysis	Policies Devices	Objects	Integration			Deploy Q 💕 🌣 🔕 admin 🔤 🐯 SECURE
Filter All Certificates	•							Adr
Name	Domain	Enroliment Type	Identity Certificate Expiry		CA Certificate Expiry	Status		
V == FTD								<u>۵</u>
1000				Identity	Certificate		0	± 0 C 🗑
							-1	± @ C @
				State Seria	us : Available al Number : 65	17	- 1	± 🖉 C 🗑
2Dd-Widout-ont		Monal (CAXC)	Det 10, 2005	 Issue C D Issue C O O Sign Assign Assign Assign Valid Valid CRL 	ed By : N: (G: G: G: H: 4:Kos bool H: 6:Key Type : RSA (2048 bits) tainer Agarithm : RSA (2048 bits) tainer Agar	Сом		

3. 정책을 저장합니다.

4. 신규 애플리케이션 그룹 및/또는 신규 애플리케이션을 생성합니다.

- 애플리케이션은 SAML 인증, 인터페이스 액세스, 침입 및 악성코드와 파일 정책을 사용하여 사설 웹 애플리케이션을 정의합니다.
- 애플리케이션 그룹을 사용하면 여러 애플리케이션을 그룹화하고 SAML 인증, 인터페이스 액 세스 및 보안 제어 설정과 같은 공통 설정을 공유할 수 있습니다.

이 예에서는 두 개의 서로 다른 애플리케이션 그룹과 두 개의 서로 다른 애플리케이션이 구성됩니 다. 하나는 Duo에서 애플리케이션을 인증하기 위한 것입니다(테스트 FMC 웹 UI). 다른 하나는 Microsoft Entra ID(CTB 웹 UI)에서 애플리케이션을 인증하기 위한 것입니다.

애플리케이션 그룹 구성

애플리케이션 그룹 1: 듀오를 IdP로 사용

a. 애플리케이션 그룹 이름을 입력하고 다음을 클릭하여 SAML SP(서비스 공급자) 메타데이터를 표시합니다.

Add Application Group

An	Application Group allows	s you to group multiple Applications and share aut	nentication, security zone, and threat configurations.
1	Application Group Name	External_Duo	Edit
2	SAML Service Provider The service provider's m metadata file as required	(SP) Metadata netadata for the Application Group are dynamically d for use in your IdP.	generated and cannot be modified. Copy or download the SP
	Entity ID https://	/External_Duo/saml/sp/metadata	Сору
	Assertion Consumer Ser https://	vice (ACS) URL External_Duo/+CSCOE+/sami/sp/acs?tgname=	Copy
3	SAML Identity Provider	(IdP) Metadata	IVEX
(4) 	Re-Authentication Inter	rval	
5	Security Zones and Sec	curity Controls	
			Cancel Finish

b. SAML SP 메타데이터가 표시되면 IdP로 이동하여 새 SAML SSO 애플리케이션을 구성합니다.

c. Duo에 로그인하여 Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다.

					Q Search	Account	Энеір Д
Dashboard		Dashboard > Applications				-	
Device Insight	~	Applicatio	ns				Protect an Application
Policies	~					X	
Applications	^	Manage your up	date to the new Universal Prompt experienc	e, all in one place.			
Protect an Application		See My Progress	Get More Information 🖸				
Authentication Pr	roxy				0	_	
Single Sign-On	~	11 All Applications	0 Fact of Support				
Users	~		unne en songegrens				
Groups	~					Export ~ Q Search	
Endpoints	~	Name -	Туре	Acc	elication Policy	Group Policies	

0 ×

d. Generic SAML Service Provider(일반 SAML 서비스 제공자)를 찾고 Protect(보호)를 클릭합니다.

-dudu DUO		Q Search	Account
Dashboard	Databased > Accelerations > Protect an Application Protect an Application		
Policies V	generic		
Applications ^	Application	Protection Type	
Protect an Application	Dette Auth API	2FA	Documentation Cf Protect
Authentication Proxy Single Sign-On ~	Generic OIDC Relying Party	2FA with SSO hosted by Duo (Single Sign-On)	Documentation Cf Protect
Users ~ Groups ~	Generic SAML Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation (f Protect

e. Secure Firewall에서 컨피그레이션을 계속 진행해야 하므로 IdP에서 인증서 및 SAML 메타데이 터를 다운로드합니다.

f. ZTNA 애플리케이션 그룹(단계 a에서 생성됨)에서 Entity ID 및 Assertion Consumer Service(ACS) URL을 입력합니다.

Dashboard	Dashboard > Applications > Generic SAML Service Provider - Single Sign-On 1					
		Generic SAM	L Service Provider - Single Sign-On 1			
Device Insight	~	See the Generic SSO documen	tation ⊑ to integrate Duo into your SAML-enabled service provider.			
Policies	~					
Applications	~	Metadata				
		Entity ID	https://sso!/metadata	Сору		
Protect an Application		Single Sign-On URL	https://sso-8(//sso	Сору		
Authentication P	roxy	Single Log-Out URL	https://sso-4 /slo	Сору		
Single Sign-On	~	Metadata URL	https://sso-8 /metadati	Сору		
Groups	~	Certificate Fingerprin	ts			
Endpoints	~	SHA-1 Fingerprint	9E:5 5C	Сору		
2FA Devices	~	SHA-256 Fingerprint	7:85 : E9:52	Сору		
Administrators	~	Downloads				
Trusted Endpoints		Certificate	Download certificate Expires: 01-19-2038			
Trust Monitor	~	SAML Metadata	Download XML			
Reports	~	Service Provider				
Settings		Metadata Discovery	None (manual input)			
Billing	~	😭 Early Access				
You're using the new Admin Panel menu a	v nd					
left-side navigation.		Entity ID *	https://///External_Duo/saml/sp/metadata			
Temporarily switch	to		The unique identifier of the service provider.			
the old experience			······	G		
		Assertion Consumer Service (ACS) URL *	https:// /External_Duo/+CSCOE+/saml/sp/ac	_90		
			+ Add an ACS URL			

g. 특정 요구 사항에 따라 애플리케이션을 편집하고 원하는 사용자만 애플리케이션에 액세스할 수 있도록 허용한 후 Save(저장)를 클릭합니다.

Туре	Generic SAML Service Provider - Single Sign-On
Name	External Applications ZTNA Duo Push users will see this when approving transactions.
Self-service portal	Let users remove devices, add new devices, and reactivate Duo Mobile See Self-Service Portal documentation [2]. To allow Duo to notify users about self-service portal activity, select Settings > Notifications
Username normalization	Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your authentication source to modify this configuration. Controls if a username should be altered before trying to match them with a Duo user account.
Voice greeting	Welcome to Duo.
Notes	For internal use. Maximum 512 characters.
Administrative unit	Assign administrative unit
Permitted groups	Only allow authentication from users in certain groups Select groups When unchecked, all users can authenticate to this application.
Allowed Hostnames	Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported. Get more information C
	Save

h. FMC로 다시 이동하고 IdP에서 다운로드한 파일을 사용하여 애플리케이션 그룹에 SAML IdP 메 타데이터를 추가합니다. An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

Name	External_Duo		
SAML Service Provider (SP) Metadata			
Entity ID Assertion Consumer Service (ACS) URL	https:// https://	'External_Duo/saml/sp/metadata 'External_Duo/+CSCOE+/saml/sp/acs?tgname=D	
SAML Identity Provider (IdP) Metadata			
Import or enter the IdP metadata. If IdP metad	lata is not currently avail	able, you can skip this step and configure it later.	
Import IdP Metadata			
Manual Configuration			
Configure Later			
Import IdP Metadata			
		_	
	t Drag and drop	your file here	
	or sele	ct file	
	External Applications ZT	NA - IDP Metadata.xml	
https://sso-8		N	
Single Sign-On URL*		N	
https://sso-c			
IdP Certificate			
MIIDDTC	/DQYJK	oZI	
			Ne
		Cancel	Fini

i. Next(다음)를 클릭하고 요구 사항에 따라 Re-Authentication Interval(재인증 간격) 및 Security Controls(보안 제어)를 구성합니다. 요약 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.

Add Application Group

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

0 ×

Name External_Duo SAML Service Provider (SP) Metadata https://:External_Duo/saml/sp/metadata Assertion Consumer Service (ACS) URL https://:External_Duo/+CSCOE+/saml/sp/acs?tgname=D SAML Identity Provider (IdP) Metadata External_Duo/+CSCOE+/saml/sp/acs?tgname=D SAML Identity Provider (IdP) Metadata External_Duo-1697063490514 Re-Authentication Interval External_Duo-1697063490514 Re-Authentication Interval 1440 minutes Security Zones and Security Controls Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
SAML Service Provider (SP) Metadata Entity ID https://:External_Duo/saml/sp/metadata Assertion Consumer Service (ACS) URL https://:External_Duo/+CSCOE+/saml/sp/acs?tgname=D SAML Identity Provider (IdP) Metadata External_Duo/+CSCOE+/saml/sp/acs?tgname=D Entity ID https://ssc Entity ID https://ssc Single Sign=On URL https://ssc IdP Certificate External_Duo-1697063490514 Re-Authentication Interval External_Duo-1697063490514 Recourty Zones and Security Controls External_Outerial (Outside) Intrusion Policy Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
Entity ID https://: External_Duo/saml/sp/metadata Assertion Consumer Service (ACS) URL https://: External_Duo/+CSCOE+/saml/sp/acs?tgname=D SAML Identity Provider (IdP) Metadata External_Duo/+CSCOE+/saml/sp/acs?tgname=D Entity ID https://ssc Single Sign-On URL https://ssc IdP Certificate External_Duo-1697063490514 Re-Authentication Interval 1440 minutes Security Zones and Security Controls Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	E
Assertion Consumer Service (ACS) URL https://: External_Duo/+CSCOE+/saml/sp/acs?tgname=D SAML Identity Provider (IdP) Metadata Entity ID Entity ID https://ssc Single Sign-On URL https://ssc IdP Certificate External_Duo-1697063490514 Re-Authentication Interval Timeout Interval 1440 minutes Security Zones and Security Controls Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
SAML Identity Provider (IdP) Metadata Entity ID https://ssc Single Sign-On URL https://ssc IdP Certificate External_Duo-1697063490514 Re-Authentication Interval Timeout Interval 1440 minutes Security Zones and Security Controls Security Zones Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
Entity IDhttps://sscSingle Sign-On URLhttps://sscIdP CertificateExternal_Duo-1697063490514Re-Authentication Interval1440 minutesTimeout Interval1440 minutesSecurity Zones and Security ControlsInherited: (Outside)Intrusion PolicyInherited: (None)Variable SetInherited: (None)Malware and File PolicyInherited: (None)	F
Single Sign-On URL IdP Certificatehttps://sscIdP CertificateExternal_Duo-1697063490514Re-Authentication IntervalTimeout Interval1440 minutesSecurity Zones and Security ControlsSecurity ZonesInherited: (Outside)Intrusion PolicyInherited: (None)Variable SetInherited: (None)Malware and File PolicyInherited: (None)	
IdP Certificate External_Duo-1697063490514 Re-Authentication Interval Image: Comparison of Comparison o	
Re-Authentication Interval 1440 minutes Timeout Interval 1440 minutes Security Zones and Security Controls Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
Timeout Interval 1440 minutes Security Zones and Security Controls Inherited: (Outside) Security Zones Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	ļ
Security Zones and Security Controls Security Zones Inherited: (Outside) Intrusion Policy Inherited: (None) Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
Security ZonesInherited: (Outside)Intrusion PolicyInherited: (None)Variable SetInherited: (None)Malware and File PolicyInherited: (None)	
Intrusion PolicyInherited: (None)Variable SetInherited: (None)Malware and File PolicyInherited: (None)	
Variable Set Inherited: (None) Malware and File Policy Inherited: (None)	
Malware and File Policy Inherited: (None)	

응용 프로그램 그룹 2: Microsoft Enterprise ID(Azure AD)를 IdP로 사용

a. 애플리케이션 그룹 이름을 입력하고 다음을 클릭하여 SAML SP(서비스 공급자) 메타데이터를 표시합니다.

Add Application Group

An Application Group allows you to group multiple Applications and share authen	tication, security zone, and threat configurations.
---	---

1	Application Group		Edit
	Name	Azure_apps	
2	SAML Service Provide The service provider's	er (SP) Metadata metadata for the Application Group are dynamically	generated and cannot be modified. Copy or download the SP
	metadata file as require	ed for use in your IdP.	
	Entity ID		
	https://	/Azure_apps/saml/sp/metadata	Сору
	Assertion Consumer Se	ervice (ACS) URL	
	https://:	Azure_apps/+CSCOE+/saml/sp/acs?tgname=E	Сору
	Download SP Metac	lata	Next
3	SAML Identity Provide	r (IdP) Metadata	
4	Re-Authentication Inte	erval	
5	Security Zones and Se	ecurity Controls	
			Cancel Finish

b. SAML SP 메타데이터가 표시되면 IdP로 이동하여 새 SAML SSO 애플리케이션을 구성합니다.

c. Microsoft Azure에 로그인하고 Enterprise Applications(엔터프라이즈 애플리케이션) > New Application(새 애플리케이션)으로 이동합니다.

	∠ Search resources, services, and docs (G+/)
Home > Enterprise applications	
Enterprise applicati	ons All applications
«	🕂 New application 🕐 Refresh 🚽 Download (Export) 🚺 Preview info 💷 Columns 🔤 Preview features 🖗 Got feedback?
Overview	
() Overview	View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.
🗙 Diagnose and solve problems	The list of applications that are maintained by your organization are in application registrations.
Manage	P Search by application name or object ID Application type == Enterprise Applications X Application ID starts with X 4 Add filters
All applications	77 applications found
Application proxy	Name ↑↓ Object ID Application ID Homepage URL Created on
* • • •	the second se

0 ×

d. Create your own application(자체 애플리케이션 생성) > Enter the name of application(애플리케이션 이름 입력) > Create(생성)를 클릭합니다.

Microsoft Azure	${\cal P}$ -Search resources, services, and docs (G+/)	D & C @ 0 R
Home > Enterprise applications All applications > Browse Microsoft Entra Gallery		Create your own application ×
+ Create your own application R Got feedback? The Microsoft Entra App Gallery is a catalog of thousands of apps that make it ear	y to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Galk	Got feedback? If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.
P Search application Single Sign-on : All	nave developed into the Microsoft Entra Callery for other organizations to discover and use, you can the a request using the User Account Management : All Categories : All	What's the name of your app? Zero Trust FTD
Contract () in the		What are you looking to do with your application? Configure Application Proxy for secure remote access to an on-premises application Register an application to integrate with Microsoft Entra ID (App you're developing) Integrate any other application you don't find in the gallery (Non-gallery)

e. 애플리케이션을 열고 Assign users and groups(사용자 및 그룹 할당)를 클릭하여 애플리케이션 에 액세스할 수 있는 사용자 및/또는 그룹을 정의합니다.



f. Add user/group(사용자/그룹 추가) > Select the required users/groups(필요한 사용자/그룹 선택) > Assign(할당)을 클릭합니다. 올바른 사용자/그룹을 할당했으면 Single sign-on을 클릭합니다.

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zero Trust FTD

<u>a</u> Zero Trust FTD U	🔁 Zero Trust FTD Users and groups						
Enterprise Application	1						
u Overview	+ Add user/group / Edit assignment 🔲 Remove	[2] Update credentials [3] □ □ □ □ Columns [2] Columns [2]					
Deployment Plan	1 The application will appear for assigned users within My Apps.	Set 'visible to users?' to no in properties to prevent this. \rightarrow					
X Diagnose and solve problems	Assign users and groups to app-roles for your application here. T	o create new app-roles for this application, use the application registration.					
Manage	· ····ð. · ··· ð. · · b. · · · b. · · · · · · · · · · ·						
Properties	First 200 shown, to search all users & gro						
A Owners	Display Name	Object Type					
alpha Roles and administrators	A Angel	101					
Users and groups	FG Fernando	1.00					
∋ Single sign-on							

g. Single sign-on 섹션에서 SAML을 클릭합니다.



h. 메타데이터 파일 업로드를 클릭하고 서비스 공급자(보안 방화벽)에서 다운로드한 XML 파일을 선택하거나 ZTNA 애플리케이션 그룹(단계 a에서 생성됨)에서 엔티티 ID 및 어설션 소비자 서비스 (ACS) URL을 수동으로 입력합니다.

Home > Enterprise applications | All applications > Zero Trust FTD

Zero Trust FTD	SAML-based Sign-on	
Enterprise Application		

EIIU	erprise Application						
		≪ <u></u> ⊼ ∪	pload metadata file 🏷 Change single sign-on	mode 🗮 Test this application 🛛 🖗 Got feedback?			
ц,	Overview						
۵	Deployment Plan	Set up Single Sign-On with SAML					
×	Diagnose and solve problems	An SSO	implementation based on federation protocols i	mproves security, reliability, and end user experiences and	is easier to		
Ma	nage	implem	ent. Choose SAML single sign-on whenever poss	ible for existing applications that do not use OpenID Conr	ect or OAuth. Learn		
		more.					
ш	Properties	Read to	he configuration guide 🖙 for help integrating Ze	ro Trust FTD.			
24	Owners	0	Desis CAMU Configuration				
2,	Roles and administrators	Ť	Basic SAML Configuration		🖉 Edit		
24	Users and groups		Identifier (Entity ID) Reply URL (Assertion Consumer Service URL)	https:// /Azure_apps/saml/sp/metadata https:// /Azure_apps/+CSCOE+/saml/sp	n/		
Э	Single sign-on		Reply one (Assertion consumer service one)	acs?tgname=DefaultZeroTrustGroup			
Ф	Provisioning		Sign on URL Relay State (Ontional)	Optional Optional			
-	Application prove		Logout Url (Optional)	Optional			
Ĩ	Application proxy						
9	Self-service	2					
	Custom security attributes		Attributes & Claims		🖉 Edit		
Sec	urity		givenname	user.givenname			
_		-	surname	user.surname			
•	Conditional Access		emailaddress	user.mail			
÷.	Permissions		Unique User Identifier	user.userprincipalname			
۹	Token encryption						
Act	ivity	3	SAML Certificates				
Э	Sign-in logs	_	Token signing certificate		A series		
66	Usage & insights		Status	Active	Edit		
_			Thumbprint				
	Audit logs		Notification Email				
ů	Provisioning logs		App Federation Metadata Url		2		
š≡	Access reviews		Certificate (Base64)	Download	_		
-			Certificate (Raw)	Download			
Iro	ubleshooting + Support		receration metadata XML	Download			
2	New support request		Verification certificates (optional)		8		
			Required	No	Edit		
			Active	0			
			Expired	0			
			Set up Zero Trust FTD				
			You'll need to configure the application to line	k with Microsoft Entra ID.			
			Login URL	https://l	2		
			Microsoft Entra Identifier	https://:	2		
			Logout URL	https://l	5		
					_		

i. FMC로 다시 이동하여 IdP에서 다운로드한 메타데이터 파일을 사용하여 SAML IdP 메타데이터를 애플리케이션 그룹 2로 가져오거나 필요한 데이터를 수동으로 입력합니다.

Add Application Group

An	Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.	
\bigcirc	Application Group	Edit
ĭ	Name Azure_apps	
2	SAML Service Provider (SP) Metadata	Edit
	Entity ID https://. /Azure_apps/saml/sp/metadata	
	SAMI Identity Provider (IdD) Metadata	
	Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.	
ſ	Import IdP Metadata	
ľ		
	Manual Configuration	
	Configure Later	
	Import IdP Metadata	
	$\overline{\uparrow}$	1
	Drag and drop your file here	Ì
	Zero Trust FTD.xml	ł
		!
	https:/	
	Single Sign-On LIDL*	
	https://	
	IdP Certificate	
	MIIC8DCCAdigAwIBAgIQdTt7Lwlj7aRGm1m212dU/DANBgkqhkiG9w0B	
	Ne	xt
4	Re-Authentication Interval	
(5)	Security Zones and Security Controls	

j. Next(다음)를 클릭하고 요구 사항에 따라 Re-Authentication Interval(재인증 간격) 및 Security Controls(보안 제어)를 구성합니다. 요약 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.

Cancel

Add A	application Group			@ ×
An A	opplication Group allows you to group multiple	Applications and share a	authentication, security zone, and threat configurations.	
1 A	Application Group			Edit
	Name	Azure_apps		
(2) \$	SAML Service Provider (SP) Metadata			Edit
	Entity ID Assertion Consumer Service (ACS) URL	https:// https://	/Azure_apps/saml/sp/metadata /Azure_apps/+CSCOE+/saml/sp/acs?tgname=Def	
(3) \$	SAML Identity Provider (IdP) Metadata			Edit
	Entity ID Single Sign-On URL IdP Certificate	https:// https://		
(4) R	Re-Authentication Interval			Edit
	Timeout Interval	1440 minutes		
5 5	Security Zones and Security Controls			Edit
	Security Zones Intrusion Policy Variable Set Malware and File Policy	Inherited: (Outside) Inherited: (None) Inherited: (None) Inherited: (None)		
			Cancel	Finish

애플리케이션 구성

애플리케이션 그룹이 생성되었으므로 애플리케이션 추가를 클릭하여 원격으로 보호 및 액세스할 애플리케이션을 정의합니다.

1. 애플리케이션 설정을 입력합니다.

a) 애플리케이션 이름: 구성된 애플리케이션의 식별자.

b) 외부 URL: 공용/외부 DNS 레코드에 있는 애플리케이션의 게시된 URL. 사용자가 애플리케이 션에 원격으로 액세스하기 위해 사용하는 URL입니다.

c) 애플리케이션 URL: 애플리케이션의 실제 FQDN 또는 네트워크 IP. 보안 방화벽에서 애플리 케이션에 연결하기 위해 사용하는 URL입니다.

✤ 참고: 기본적으로 외부 URL은 애플리케이션 URL로 사용됩니다. 다른 애플리케이션 URL을 지정하려면 이 확인란의 선택을 취소합니다.

(d) 애플리케이션 인증서: 액세스할 애플리케이션의 인증서 체인 및 개인 키(FMC 홈 페이지 > Objects > Object Management > PKI > Internal certs에서 추가)

e) IPv4 NAT 소스(선택 사항): 원격 사용자의 소스 IP 주소는 패킷을 애플리케이션에 전달하기 전에 선택한 주소로 변환됩니다(IPv4 주소를 갖는 호스트 및 범위 유형 네트워크 객체/객체 그룹만 지원됨). 이는 애플리케이션이 Secure Firewall을 통해 원격 사용자에게 다시 경로를 제공하도록 구 성할 수 있습니다

f) 응용 프로그램 그룹(선택 사항): 이 응용 프로그램을 기존 응용 프로그램 그룹에 추가하여 구 성된 설정을 사용하려면 선택합니다.

이 예에서 ZTNA를 사용하여 액세스할 수 있는 애플리케이션은 테스트 FMC 웹 UI 및 Secure Firewall 뒤에 있는 CTB의 웹 UI입니다.

애플리케이션의 인증서는 Objects(개체) > Object Management(개체 관리) > PKI > Internal certs(내부 인증서)에서 추가해야 합니다.

Ø

Add Known Internal Certificate

Name:		
ao-fmc-ztna.cisco.local		
Certificate Data or, choose a file: Browse		
BEGIN CERTIFICATE		_
		т
		G XY
Key or, choose a file: Browse		
BEGIN <u>RSA</u> PRIVATE KEY		
Encrypted, and the password is:		
	Cancel	Save

🦠 참고: ZTNA로 액세스할 각 애플리케이션에 대한 모든 인증서를 추가해야 합니다.

인증서가 내부 인증서로 추가되었으면 나머지 설정을 계속 구성합니다.

이 예에 대해 구성된 애플리케이션 설정은 다음과 같습니다.

응용 프로그램 1: FMC 웹 UI 테스트(응용 프로그램 그룹 1의 멤버)

	Enabled
Application Settings	
Application Name*	
FMC	
External URL* 🕧	
https://ao-fmc-ztna.cisco.local	
Application URL (FQDN or Network IP)*	
https://ao-fmc-ztna.cisco.local	
Use External URL as Application URL	
By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443	
Application Certificate* 🕕	
ao-fmc-ztna.cisco.local \times \checkmark +	
IPv4 NAT Source 📵	
Select V +	
Application Group	
External_Duo X V	
SAML Service Provider (SP) Metadata	
SAML Identity Provider (IdP) Metadata	
Re-Authentication Interval	
Security Zones and Security Controls	

응용 프로그램이 응용 프로그램 그룹 1에 추가되었으므로 이 응용 프로그램에 대해 나머지 설정이 상속됩니다. 보안 영역 및 보안 제어를 다른 설정으로 재정의할 수 있습니다.

구성된 애플리케이션을 검토하고 Finish(마침)를 클릭합니다.

애플리케이션 2: CTB 웹 UI(애플리케이션 그룹 2의 멤버)

이 응용 프로그램에 대한 구성 요약은 다음과 같습니다.

		Enabled	
1 Application Settings			Edit
Application Name	СТВ		
External URL	https://ao-ctb.cisco.local		
Application URL	https://ao-ctb.cisco.local		
IPv4 NAT Source	ZTNA_NAT_CTB		
Application Certificate	ao-ctb.cisco.local		
Application Group	Azure_apps		
2 SAML Service Provider (SP) Metada	ata		
Configurations are derived from App	lication Group 'Azure_apps'		
3 SAML Identity Provider (IdP) Metad	ata		
Configurations are derived from App	lication Group 'Azure_apps'		
Re-Authentication Interval			
Configurations are derived from App	lication Group 'Azure_apps'		
Security Zones and Security Control	bls		Edit
Security Zones	Inherited: (Outside)		
Intrusion Policy	Inherited: (None)		
Variable Set	Inherited: (None)		
Malware and File Policy	Inherited: (None)		
		Cancel	Finish

참고: 이 애플리케이션의 경우 네트워크 객체 "ZTNA_NAT_CTB"가 IPv4 NAT 소스로 구성되었습니다. 이 구성에서는 패킷을 애플리케이션에 전달하기 전에 원격 사용자의 소스 IP 주소 가 구성된 객체 내의 IP 주소로 변환됩니다. 이는 애플리케이션(CTB) 기본 경로가 보안 방화벽이 아닌 게이트웨이를 가리키므로 반환 트 래픽이 원격 사용자에게 전송되지 않기 때문에 구성되었습니다. 이 NAT 컨피그레이션을 통해서브넷 ZTNA_NAT_CTB가 보안 방화벽을 통해 연결할 수 있도록 애플리케이션에 고정 경로가 구성되었습니다.

애플리케이션이 구성되면 해당 애플리케이션 그룹 아래에 표시됩니다.

ZTN	A-TAC 🖌									c	Targ aroups: 3	peted: 1 c	levice
	Applications	Setti	ngs										
Bulk	Actions	~	Q, Filter	by Name, IdP SAML missing, Enabled/Disabled						Add Application Group	Add	1 Applica	tion
	Name			External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware a	and File Policy Er	abled		
\sim	Azure_apps (1 Applicat	ion)			https://sts.v	Outside (Inherited)	None (Inherited)	None (In	herited)		* /	÷.
\bigcirc	CTB			https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (In	herited) Tr	ue	* /	÷.
\sim	External_Duo	(1 Applic	ation)			https://sso-	Outside (Inherited)	None (Inherited)	None (In	herited)		* /	Ť
	FMC			https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (In	herited) Tr	ue	21	

마지막으로, 변경 사항을 저장하고 컨피그레이션을 구축합니다.

다음을 확인합니다.

컨피그레이션이 실행되면 원격 사용자가 외부 URL을 통해 애플리케이션에 연결할 수 있으며, 해당 IdP에서 허용하면 애플리케이션에 액세스할 수 있습니다.

애플리케이션 1

1. 사용자가 웹 브라우저를 열고 애플리케이션 1의 외부 URL로 이동합니다. 이 경우 외부 URL은 https://ao-fmc-ztna.cisco.local/입니다<u>.</u>

✤ 참고: 외부 URL 이름은 구성된 보안 방화벽 인터페이스의 IP 주소로 확인되어야 합니다. 이 예에서는 외부 인터페이스 IP 주소(192.0.2.254)로 확인됩니다

2. 새 액세스이므로 사용자는 애플리케이션에 대해 구성된 IdP 로그인 포털로 리디렉션됩니다.

$\leftarrow \rightarrow C$	O A https://sso-		ំ 🕁	⊠ ⊜	ර ≡
		rescore Single Sign-On a edt Password Log in Secured by Duo			

3. 사용자에게 MFA 푸시를 보냅니다(IdP에 구성된 MFA 방법에 따라 다름).

Are you logging in to External Applications ZTNA?

④ 1:13 p.m.

2. 새 액세스이므로 사용자는 애플리케이션에 대해 구성된 IdP 로그인 포털로 리디렉션됩니다.

← → C iii login.microsoftonline.com/	ten hann fei fei eine fei fei fei fei fei fei fei fei fei fe	
	Microsoft	
	Sign in	
	rgt/dites or	
	Next	
	℃ Sign-in options	
← → C ▲ login.microsoftonline.com/login.srf		
← → C ▲ login.microsoftonline.com/login.srf		
← → C ▲ login.microsoftonline.com/login.srf		
← → C ▲ login.microsoftonline.com/login.srf		
← → ℃ is login.microsoftonline.com/login.srf		
← → C a login.microsoftonline.com/login.srf		
← → C (a login.microsoftoniine.com/login.srf		
← → C (à login.microsoftonline.com/login.srf		
← → C (a login.microsoftonline.com/login.srf		
← → C a login.microsoftonline.com/login.srf		
← → C a login.microsoftonline.com/login.srf	Microsoft	
← → C a login.microsoftonline.com/login.srf	Microsoft	
← → C a login.microsoftonline.com/login.srf	Microsoft	
← → C a login.microsoftonline.com/login.srf	Microsoft Approve sign in request	
← → C a login.microsoftonline.com/login.srf	Microsoft Approve sign in request Open your Authenticator app, and enter the Deep your Authenticator app, and enter the Deep your Authenticator app, and enter the	
C ● login.microsoftonline.com/login.srf	Microsoft Microsoft Microsoft Deprove sign in request Open your Authenticator app, and enter the number shown to sign in.	
C e login.microsoftonline.com/iogin.srf	Microsoft Microsoft Approve sign in request On your Authenticator app, and enter the number shown to sign in. 67	
€ → C a login.microsoftonline.com/login.srf	Microsoft Deprove sign in request More sign in the sign in. 167	
€ → C a login.microsoftonline.com/login.srf	 Microsoft Approve sign in request Open your Authenticator app, and enter the number shown to sign in. 67 	
	 Microsoft Approve sign in request On your Authenticator app, and enter the numbers shown to sign in. On your Authenticator app, and enter the numbers in your app? Make sure to upgrade to the last version. 	
C login.microsoftonline.com/login.srf	<text><text><text><text><text><text></text></text></text></text></text></text>	
	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	
C Iogin.microsoftonline.com/login.srf	<text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text>	
C Iogin.microsoftonline.com/login.srf	<text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text>	
	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	
 C login.microsoftonline.com/login.srf 	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	
C A Iogin.microsoftonline.com/login.srt	<image/> <section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	

3. 사용자에게 MFA 푸시를 보냅니다(IdP에 구성된 MFA 방법에 따라 다름).

컨피그레이션에서 문제가 발생한 시점을 표시하여 사용자의 문제 해결 프로세스를 용이하게 하도록 설계되었습니다

• 진단을 통해 전반적인 분석(정상 여부 확인)을 제공하며 문제를 해결하기 위해 분석할 수 있는 자세한 로그를 수집합니다.

애플리케이션별 진단을 사용하여 다음을 탐지합니다.

- DNS 관련 문제
- 잘못된 컨피그레이션(예: 소켓 열리지 않음, 분류 규칙, NAT 규칙)
- 제로 트러스트 액세스 정책의 문제
- 인터페이스 관련 문제(예: 인터페이스가 구성되지 않았거나 인터페이스가 다운됨)

검색할 일반 진단:

- 강력한 암호 라이센스가 활성화되지 않은 경우
- 애플리케이션 인증서가 유효하지 않은 경우
- 인증 방법이 기본 터널 그룹에서 SAML로 초기화되지 않은 경우
- HA 및 클러스터 대량 동기화 문제
- 토큰 또는 암호 해독 관련 문제를 진단하기 위해 snort 카운터에서 통찰력을 얻습니다.
- 소스 변환의 PAT 풀 소모 문제

진단을 실행하려면

1. 각 ZTNA 애플리케이션에 대해 표시되는 진단 아이콘으로 이동합니다.

A	pplications	Settings								
Bulk	Actions	V Q. Filter	by Name, IdP SAML missing, Enabled/Disabled					Add Application G	iroup	Add Application
	Name		External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Mahware and File Policy	Enabled	
\sim	Azure_apps (1	Application)				Outside (Inherited)	None (Inherited)	None (Inherited)		
	CTB		No. of Concession, Name	100 C		Outside (Inherited)	None (Inherited)	None (Inherited)	True	*/1
\sim	External_Duo	(1 Application)			-	Outside (Inherited)	None (Inherited)	None (Inherited)		Diagnostics
	FMC					Outside (Inherited)	None (Inherited)	None (Inherited)	True	*/=

2. 장치를 선택하고 실행을 클릭합니다.

Diagnostics:	CTR.
rear and a second second	2010/07/1

Belect 🗸 Run	
= FTD	

Cancel

3. 보고서의 결과를 조회합니다.

Diagnostics: CTB		×
Select Device	Run	
Report Logs		ß

- > Ø Application Specific Validation
- > O General Validation

Cancel

FTD CLI에서는 show 및 clear 명령을 사용하여 제로 트러스트 컨피그레이션을 보고 통계와 세션 정보를 표시할 수 있습니다.

<#root>

firepower# show running-config zero-trust

application Show application configuration information application-group Show application group configuration | Output modifiers <cr>

firepower# show zero-trust

sessions Show zero-trust sessions statistics Show zero-trust statistics

firepower# show zero-trust sessions

```
applicationshow zero-trust sessions for applicationapplication-groupshow zero-trust sessions for application groupcountshow zero-trust sessions countusershow zero-trust sessions for userdetailshow detailed info for the session|Output modifiers<Cr>
```

firepower# clear zero-trust

sessions Clear all zero-trust sessions statistics Clear all zero-trust statistics

firepower# clear zero-trust sessions

```
application Clear zero-trust sessions for application
user Clear zero-trust sessions for user
<Cr>
```

제로 트러스트 및 webvpn 모듈 디버그를 활성화하려면 Lina 프롬프트에서 다음 명령을 사용합니다

- firepower# 디버그 제로 트러스트 255
- firepower 번호 디버그 webvpn 요청 255
- firepower 번호 디버그 webvpn 응답 255
- firepower 번호 디버그 webvpn saml 255

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계 약이 필요합니다. <u>Cisco Worldwide Support Contacts</u>.
- <u>여기서</u> Cisco VPN Community를 방문할 수도 <u>있습니다</u>.

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 번 역 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.