在安全防火牆上配置零信任遠端訪問部署

目錄
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
網路圖表
<u>先決條件配置</u>
配置應用程式組
<u>應用組1:使用Duo作為IdP</u>
<u>應用程式組2:使用Microsoft Entra ID(Azure AD)作為IdP</u>
配置應用程式
<u>應用程式1:測試FMC Web UI(應用程式組1的成員)</u>
<u>應用程式2:CTB Web UI(應用程式組2的成員)</u>
<u>驗證</u>
<u>監視</u>
<u>疑難排解</u>
相關資訊

簡介

本文描述在安全防火牆上配置無客戶端零信任訪問遠端訪問部署的過程。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower Management Center (FMC)
- 基本ZTNA知識
- 基本安全斷言標籤語言(SAML)知識

採用元件

本檔案中的資訊是根據以下軟體版本:

- 安全防火牆版本7.4.1
- Firepower管理中心(FMC)版本7.4.1

- Duo作為身份提供者(IdP)
- 作為IdP的Microsoft Entra ID(以前稱為Azure AD)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

零信任訪問功能基於零信任網路訪問(ZTNA)原則。ZTNA是一種零信任安全模型,消除了隱性信任 。該模型在驗證使用者、請求上下文以及分析訪問被授予的風險後,授予最小許可權訪問許可權。

目前ZTNA的要求和限制如下:

- 受FMC 7.4.0+版(Firepower 4200系列)管理的安全防火牆版本7.4.0+支援
- 受FMC版本7.4.1+管理的安全防火牆版本7.4.1+支援(所有其他平台)
- 僅支援Web應用程式(HTTPS)。不支援要求解密豁免的場景
- 僅支援SAML IdP
- 遠端訪問需要公共DNS更新
- 不支援IPv6。不支援NAT66、NAT64和NAT46方案
- 只有啟用Snort 3後,威脅防禦功能才可用
- 受保護的Web應用程式中的所有超連結都必須具有相對路徑
- 在虛擬主機或內部負載平衡器後面運行的受保護的Web應用程式必須使用相同的外部和內部 URL
- 在單獨模式群集上不受支援
- 啟用了嚴格HTTP主機標頭驗證的應用程式不支援
- 如果應用程式伺服器託管多個應用程式並根據TLS客戶端Hello中的伺服器名稱指示(SNI)標頭 提供內容,則零信任應用程式配置的外部URL必須與特定應用程式的SNI匹配
- 僅在路由模式下支援
- 需要智慧許可證(無法在評估模式下工作)

有關安全防火牆中零信任訪問的詳細資訊和詳細資訊,請參閱<u>思科安全防火牆管理中心裝置配置指</u> <u>南7.4</u>。

設定

本文檔重點介紹ZTNA的遠端訪問部署。

在此示例場景中,遠端使用者需要訪問測試FMC和思科遙測代理(CTB)的Web使用者介面(UI),它們 託管在安全防火牆之後。訪問這些應用程式由兩個不同的IdP分別授予:Duo和Microsoft Entra ID,如下圖所示。

網路圖表



拓撲圖表

- 1. 遠端使用者需要訪問安全防火牆後託管的應用程式。
- 2. 每個應用程式在公共DNS伺服器中必須有一個DNS條目。
- 3. 這些應用程式名稱必須解析為安全防火牆外部介面的IP地址。
- 4. 安全防火牆解析為應用程式的實際IP地址,並使用SAML身份驗證對每個應用程式驗證每個使 用者。

先決條件配置

身分識別提供程式(IdP)和網域名稱伺服器(DNS)

- 必須在SAML身份提供程式(IdP)中配置應用程式或應用程式組,例如Duo、Okta或Azure AD。在此示例中,Duo和Microsoft Entra ID用作IdP。
- 在安全防火牆上配置應用程式時,會使用由IdP生成的證書和後設資料

內部和外部DNS伺服器

- 外部DNS伺服器(由遠端使用者使用)必須具有應用程式的FQDN條目,並解析到安全防火牆 外部介面IP地址
- 內部DNS伺服器(由Secure Firewall使用)必須具有應用程式的FQDN條目,並解析為應用程 式的實際IP地址

慿證

ZTNA策略配置需要以下證書:

- 身份/代理證書:由安全防火牆用於偽裝應用程式。此處的安全防火牆充當SAML服務提供商 (SP)。此證書必須是與專用應用程式的FQDN相匹配的萬用字元或使用者替代名稱(SAN)證書 (在預身份驗證階段代表所有專用應用程式的通用證書)
- IdP證書:用於身份驗證的IdP為定義的每個應用程式或應用程式組提供證書。必須配置此證書 ,以便安全防火牆 能夠驗證傳入SAML斷言上的IdP簽名(如果這是針對應用程式組定義的,則同一證書將用於 整個應用程式組)
- 應用證書:從遠端使用者到應用的加密流量需要由安全防火牆解密,因此,必須將每個應用的 證書鏈和私鑰新增到安全防火牆。

常規配置

要配置新的零信任應用程式,請執行以下步驟:

1. 導航到Policies > Access Control > Zero Trust Application, 然後點選Add Policy。

2. 填寫必填欄位:

a)General:輸入策略的名稱和說明。

b)域名:這是新增到DNS中的名稱,必須解析到訪問應用程式的威脅防禦網關介面。

💊 注意:域名用於為應用程式組中的所有專用應用程式生成ACS URL。

c)身份證書:這是代表預身份驗證階段的所有專用應用程式的通用證書。

注意:此證書必須是與專用應用程式的FQDN相匹配的萬用字元或使用者替代名稱(SAN)證書。

d)Security Zones: 選擇用於管理專用應用程式的outside或/和inside zones。

e)全域性埠池:此池中的唯一埠分配給每個專用應用程式。

f)安全控制(可選):選擇是否對私人申請進行檢查。

在此範例組態中,輸入以下資訊:

Policies / Access Control / Zero Trust Application Overview Analysis	Policies Devices	Objects Integration		Deploy Q 🗳 🌣 🚳 admin 🗸 🖓 SE	CURE
*) Return to Zero Trust Application Add a Zero T Zero Trust Application	rust Application Pol on Policy protects private appl	ICy income with identity based access, intrusion protection, and makeum and file inspection.	Cancel Save		
	IdP				
	General	Name* ZTNA-TAC Description			
	Domain Name	The domain name must resolve to the interfaces that are part of the security zones from which private applications are accessed. Bomain Name* Comain Name* Comain name resolves to the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed. The domain name is und to generate the ACS URE, for all private applications in an Application Group.			
	Identity Certificate	A common certificate that represents all the private applications at the pre-authentication stage. Certificate* ZTMA-Wildcard-cert × ✓ + This certificate must be a wildcard or Subject Atemative Name (SAN) certificate that must be the FOCN of the private applications.			
	Security Zones	The access to private applications is regulated through security zones. Choose outside orland inside zones through which the private applications are regulated. Security Zones* Security Zones* V V Outside x X V +			
	Gilobal Port Pool	Unique port from this pool is assigned to each private application. Port Range* 20000-22000 Range: (1024-65535) © Enure a sufficient range is previded to accommodate all private applications. Do not share these ports in NAT or other configurations.			
	Security Controls (Optional)	Private applications can be subject to inspection using a selected intrusion or Malware and File policy; Intrusion Policy Variable Set None V + Makware and File Policy None V · · + These are default settings for all private applications. It can be eventided at an Application or Application Group level.			

在此案例中使用的身份/代理證書是與專用應用程式的FQDN匹配的萬用字元證書:

Firewall Manage Devices / Certificates	ment Center	Overview Analysis	is Policies Devic	s Objects	Integration			Deploy Q 💰 🔅 🔕	admin v dode SECURE
Filter All Certificates	*								Add
Name	Domain	Enrolment Type	Identity Certificate Expiry		CA Certificate Expiry	Status			
V mm FTD									a
				Identi	ty Certificate		0		± ₽ ⊂ ₩
									± 🖉 C 🗑
				• s	tatus : Available erial Number : 65	17			± @ C 🗑
2004-0012-245-245		Down (CALL)	Cu 10, 2025	- h	sued By : CY: _ discalocal DC: DC: DC: CY: _ discalocal OU: TAC OU: TAC OU: TAC OU: TAC OU: TAC ST: CHECKEY Type : R5A (2048 bms) ignature Agorithm : R5A-94X384 ssociated Trustgionts : ZTMA-Millioard-eert allef From : 225942 UTC October 11 2023 allef To: 225942 UTC October 10 2025 RL Distribution Points :				1. 17 C 1

4.建立新的應用程式組和/或新的應用程式:

- 應用定義具有SAML身份驗證、介面訪問、入侵和惡意軟體以及檔案策略的專用Web應用。
- Application Group允許您對多個應用程式進行分組,並共用通用設定,例如SAML身份驗證、 介面訪問和安全控制設定。

在此範例中,設定兩個不同的應用程式群組和兩個不同的應用程式:一個用於Duo進行驗證的應用 程式(測試FMC Web UI),另一個用於Microsoft Entra ID(CTB Web UI)進行驗證的應用程式。

配置應用程式組

應用組1:使用Duo作為IdP

a.輸入應用程式組名稱,然後按一下下一步以顯示的SAML服務提供程式(SP)後設資料。

Add	Application Group	@ ×
An	Application Group allows you to group multiple Applications and share aut	entication, security zone, and threat configurations.
1	Application Group Name External_Duo	Edit
2	SAML Service Provider (SP) Metadata	
	The service provider's metadata for the Application Group are dynamically metadata file as required 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 Service (ACS) URL	
	https:// External_Duo/+CSCOE+/saml/sp/acs?tgname=	Сору
	Download SP Metadata	Next
3	SAML Identity Provider (IdP) Metadata	
4	Re-Authentication Interval	
5	Security Zones and Security Controls	
		Cancel Finish

b.顯示SAML SP後設資料後,請轉到IdP並配置新的SAML SSO應用程式。

c.登入到Duo,然後導航到Applications > Protect an an Application。

			Q Search	Account 🛛 🔿 Help 🛛 🔤
Dashboard Device Insight	~	Databased > Applications Applications		Protect an Application
Policies Applications	~	Manage your update to the new Universal Prompt experience, all in one place.		
Protect an Application Authentication	Proxy	See My Progress Get More Information (3	•	
Single Sign-On	×	11 0 End of Support		
Groups	~			Export ~ Q Search
Endpoints	~	Name • Type	Application Policy	Group Policies

d.查詢通用SAML服務提供程式,然後按一下保護。

cuco DUO		Q Search	Account 🛛 🗍 🕐 Help	ደ •
Dashboard	Databased > Accelerations > Protect an Application Protect an Application			
Policies ~	generic			
Applications ^	Application	Protection Type		
Protect an Application	DIO Auth API	2FA	Documentation D	Protect
Authentication Proxy Single Sign-On V	Generic OIDC Relying Party	2FA with SSO hosted by Duo (Single Sign-On)	Documentation IS	Protect
Users ~ Groups ~	Generic SAML Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation Id	Protect

e.從IdP下載證書和SAML後設資料,因為在Secure Firewall上繼續配置需要該後設資料。

f.輸入ZTNA應用程式組(在步驟a中生成)的實體ID和斷言使用者服務(ACS)URL。

Dashboard	Dashboard > Applications >	Generic SAML Service Provider - Single Sign-On 1	
	Generic SA	ML Service Provider - Single Sign-On 1	
Device Insight	✓ See the Generic SSO docum	nentation 💕 to integrate Duo into your SAML-enabled service provider.	
Policies	~		
Applications		https://sen//metadati	Copy
Protect an	Entry ID	Interaute Interaute	Сору
Application	Single Sign-On URL	https://sso-8(1/sso	Сору
Authentication P	Proxy Single Log-Out URL	https://sso-i /slo	Сору
Single Sign-On	∽ Metadata URL	https://sso-8 /metadata	Сору
Users	~		
Groups	 Certificate Fingerpr 	rints	
Endpoints	SHA-1 Fingerprint	9E:5	Сору
2FA Devices	SHA-256 Fingerprint	7:85: E9:52	Сору
Administrators	 Downloads 		
Trusted Endpoints	Certificate	Download certificate Expires: 01-19-2038	
Trust Monitor	V SAML Metadata	Download XML	
Reports	✓ Service Provider		
Settings	Metadata Discovery	None (manual input)	
Billing	👻 🔮 Early Access		
You're using the new	N		
Admin Panel menu a left-side navigation.	Entity ID *	https://z /External_Duo/saml/sp/metadata	
Provide feedback		The unique identifier of the service provider.	
Temporarily switch the old experience	to		
	Assertion Consumer Service (ACS) URL *	https://. 'External_Duo/+CSCOE+/saml/sp/ac	
		+ Add an ACS URL	

g.根據您的特定要求編輯應用程式,僅允許目標使用者訪問應用程式,然後按一下儲存。

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 C. 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.使用從ldP下載的檔案導航回到FMC,並將SAML ldP後設資料新增到應用程式組。

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	data is not currently avail	able, you can skip this step and configure it later.	
Import IdP Metadata			
Manual Configuration			
Configure Later			
Import IdP Metadata			
		-	
	Drag and drop	your file here	
	or sele	<u>ct file</u>	
	External Applications ZT	NA - IDP Metadata.xml	
Entity ID*			
https://sso-8		N	
Single Sign-On URL*			
https://sso-8		N	
IdP Certificate			
MIIDDTC	/DQYJK	oZI	
			Mar
			Nex
			Field

i.按一下Next,然後根據要求設定Re-Authentication Interval和Security Controls。檢視摘要配置 ,然後按一下Finish。

Add Application Group

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

	Application Group		Edit	
1	Name	External_Duo		
2	SAML Service Provider (SP) Metadata		Edit	
Ī	Entity ID Assertion Consumer Service (ACS) URL	https://: External_Duo/saml/sp/metadata https://: External_Duo/+CSCOE+/saml/sp/acs?tgname=D		
3	SAML Identity Provider (IdP) Metadata		Edit	
	Entity ID Single Sign-On URL IdP Certificate	https://ssc https://ssc External_Duo-1697063490514		
4	Re-Authentication Interval		Edit	
	Timeout Interval	1440 minutes		
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	

應用程式組2:使用Microsoft Entra ID(Azure AD)作為IdP

a.輸入應用程式組名稱,然後按一下下一步以顯示的SAML服務提供程式(SP)後設資料。

Add Application Group

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

1	Application Group		Edit
	Name	Azure_apps	
2	SAML Service Provi	ider (SP) Metadata	
	The service provider metadata file as requ	's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the S uired for use in your IdP.	SP
	Entity ID		
	https://	Azure_apps/saml/sp/metadata Copy	
	Assertion Consumer	Service (ACS) URL	
	https://:	Azure_apps/+CSCOE+/saml/sp/acs?tgname=E Copy	
	Download SP Met	tadata	t
3	SAML Identity Provi	ider (IdP) Metadata	
4	Re-Authentication I	nterval	
5	Security Zones and	Security Controls	
		Cancel Finis	h

b.顯示SAML SP後設資料後,請轉到IdP並配置新的SAML SSO應用程式。

c.登入到Microsoft Azure,然後導航到「企業應用程式」>「新應用程式」。

	A	Search resources, services, and docs (G+/)					
Home > Enterprise applications							
Enterprise applica	Enterprise applications All applications						
Overview	≪ 🕂 New application 🕐 Refresh 🛓 Downlos	ad (Export) 1 Preview info 🗮 Columns	💀 Preview features 🛛 🕅 Got	feedback?			
() Overview	View, filter, and search applications in your organization	ation 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	Search by application name or object ID	Application type == Enterprise Applications \times	Application ID starts with $ imes$	⁺ _▼ Add filters			
All applications	77 applications found						
Application proxy	Name ↑↓ Object ID	Application ID	Homepage URL	Created on			
🏎							

d.按一下建立自己的應用程式>輸入應用程式的名稱>建立

0 ×



e.開啟應用程式,然後按一下分配使用者和組,以定義允許訪問應用程式的使用者和/或組。

Home > Enterprise applications All ap	pplications > Browse Microsoft Entra Gallery >
Enterprise Application	verview
() 	
Contraction of the second seco	Properties
U Deployment Plan	ZI Name O
X Diagnose and solve problems	Zero Trust FID
Manage	Application ID 💿
Properties	
2 Owners	
Roles and administrators	Carling Strengt
Users and groups	Getting started
Single sign-on	
Provisioning	🚴 1. Assign users and groups 🏐 2. Set up single sign on 👔 3. Provision User Accounts 🍋 4. Conditional Access
Application proxy	Provide specific users and groups access Enable users to sign into their application Automatically create and delete user Secure access to this application with a using their application are and application and application are applied and application with a performation of the application are applied and application are application are applied and application application are applied and application application are applied and application are ap
Self-service	A sign users and groups Get stated Get stated Certain a plucation Constraint and a state of Certain a plucation of the state of the state of the state of the state of the sta
Custom security attributes	
Security	
Conditional Access	S . Self service
2 Permissions	Enable users to request access to the anolicitation using their Microards Forma
Token encryption	credentials Get started
Activity	
~ 1 1 1	

f.按一下Add user/group > Select the needed users/groups > Assign。分配正確的使用者/組後,按 一下單點登入。

Home > Enterprise applications All applications > Browse Microsoft Entra Gallery > Zero Trust FTD						
Zero Trust FTD U	Zero Trust FTD Users and groups					
enceptise approaction	+ Add user/group ∅ Edit assignment ∅	Remove 🖉 Update credentials 🗮 Columns 🕅 Got feedback?				
u Overview	The application will appear for accigned upper with	a Mu Appr. Set "visible to user?" to ap in proportion to prove this \rightarrow				
Deployment Plan	The application will appear for assigned users with	n wy Apps, set visible to users: to no in properties to prevent this>				
✗ Diagnose and solve problems	X Diagnose and solve problems Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.					
Manage						
Properties	First 200 shown, to search all users & gro					
28 Owners	Display Name	Object Type				
Roles and administrators	AO Angel					
Users and groups	FG Fernando					
Single sign-on						

g.在Single sign-on部分中,按一下SAML。



h.按一下Upload metadata file 並選擇從服務提供商(Secure Firewall)下載的XML檔案,或手動從 ZTNA應用程式組輸入Entity ID和Assertion Consumer Service(ACS)URL(在步驟a中生成)。

◆ 注意:請確保也下載聯合後設資料XML或單獨下載證書(基本64),並從IdP(登入和註銷 URL和Microsoft Entra識別符號)複製SAML後設資料,因為這些內容是繼續安全防火牆上的 配置所必需的。

Home > Enterprise applications | All applications > Zero Trust FTD

Zero Trust FTD	SAML-based Sign-on	
Enterprise Application		

2.110	albuar Abburation	« 🔻	below the fill be described at the					
	Overview	Т	Upload metadata file / Change single sign-on	mode I lest this application X Got feedback?				
۵	Deployment Plan	Set	Set up Single Sign-On with SAML					
×	Diagnose and solve problems							
		An S imple	SO implementation based on federation protocols i ement. Choose SAML single sign-on whenever poss	mproves security, reliability, and end user experiences and ible for existing applications that do not use OpenID Conn	is easier to ect or OAuth. Learn			
Ma	nage	more	2.					
	Properties	Read	d the configuration guide 📑 for help integrating Ze	ro Trust FTD.				
24	Owners	•						
2,	Roles and administrators	, v	Basic SAML Configuration		🖉 Edit			
24	Users and groups		Identifier (Entity ID)	https:// /Azure_apps/saml/sp/metadata				
Э	Single sign-on		Reply URL (Assertion Consumer Service URL)	acs?tgname=DefaultZeroTrustGroup	2/			
(h)	Provisioning		Sign on URL	Optional				
Ť	Provisioning		Relay State (Optional)	Optional Optional				
10	Application proxy		Logout en (optional)	o piteriar				
0	Self-service							
	Custom security attributes	6	Attributes & Claims		🖉 Edit			
			givenname	user.givenname				
Sec	cunty		surname	user.sumame				
•	Conditional Access		emailaddress	user.mail				
-	Permissions		name Upique User Identifier	user.userprincipalname				
1			onique oser identifier	user.userprincipaniane				
Y	Token encryption							
Act	tivity		SAML Certificates					
Э	Sign-in logs		Token signing certificate		/ Edit			
άí.	Usage & insights		Status	Active	₽ Eun			
-	A		Thumbprint					
	Audit logs		Notification Email					
ů	Provisioning logs		App Federation Metadata Url		5			
¥≡	Access reviews		Certificate (Base64)	Download	_			
			Certificate (Raw)	Download				
Tro	oubleshooting + Support		Federation Metadata XML	Download				
2	New support request		Varification cartificates (ontional)					
			Required	No	🖉 Edit			
			Active	0				
			Expired	0				
		4	Set up Zero Trust FTD					
			You'll need to configure the application to line	k with Microsoft Entra ID.				
			Login URL	https://l	5			
			Microsoft Entra Identifier	https://:	5			
			Logout URL	https://l	รี			

i.使用從IdP下載的後設資料檔案或手動輸入所需資料,導航回到FMC,然後將SAML IdP後設資料 匯入到應用程式組2。

Add Application Group

An	Application Group allows you to group multiple Ap	plications and share aut	hentication, security zone, and threat configurations.	
(1)	Application Group			Edit
ĭ	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 Import or enter the IdP metadata. If IdP metadata	is not currently available	, you can skip this step and configure it later.	
[Import IdP Metadata			
	Manual Configuration			
	Onfigure Later			
	Import IdP Metadata			
		*		
		Drag and drop yo	ur file here	
		or select fi	le) yml	1
		Zelo Hustri		j
	Entity ID*			
	https:/	A. LOW DRIVE		
	Single Sign-On URL*			
	https://			
	IdP Certificate			
	MIIC8DCCAdigAwlBAglQdTt7Lwlj7aRGm1m212d / ł I : :	dU/DANBgkqhkiG9w0B		
			Nex	kt
4	Re-Authentication Interval			
5	Security Zones and Security Controls			

j.按一下下一步,然後根據要求配置重新身份驗證間隔和安全控制。檢視摘要配置,然後按一下 Finish。

Cancel

Add Application Group			0 ×
An Application Group allows you to group multip	le Applications and share	authentication, security zone, and threat configurations.	
1 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) Re-Authentication Interval			Edit
Timeout Interval	1440 minutes		
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

配置應用程式

建立應用程式組後,按一下Add Application以定義要遠端保護和訪問的應用程式。

1. 輸入應用程式設定:

a)應用程式名稱:已配置應用的識別符號。

b)外部URL:公用/外部DNS記錄中應用程式的已發佈URL。這是使用者用於遠端訪問應用程式的URL。

c)應用程式URL:應用程式的實際FQDN或網路IP。這是Secure Firewall用於訪問應用程式的URL。

✤ 注意:預設情況下,外部URL用作應用程式URL。取消選中此覈取方塊可指定其他應用程式 URL。

d)Application Certificate:要訪問的應用程式的證書鏈和私鑰(從FMC首頁>對象>對象管理> PKI >內部證書新增的)

e)IPv4 NAT源(可選):在將資料包轉發到應用程式之前,會將遠端使用者的源IP地址轉換為 所選地址(僅支援具有IPv4地址的主機和範圍型別網路對象/對象組)。可以對此進行配置,以確保 應用程式具有通過安全防火牆返回到遠端使用者的路由

f)應用程式組(可選):選擇是否將此應用程式新增到現有應用程式組,以使用為其配置的設定。

在本示例中,使用ZTNA訪問的應用程式是測試FMC Web UI和位於安全防火牆後面的CTB的Web UI。

(2)

必須在對象>對象管理> PKI >內部證書中新增應用程式的證書:

Add Known Internal Certificate

ao-fmc-ztna.cisco.local	
Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE	
	т
	G AY
Key or, choose a file: Browse	
BEGIN RSA PRIVATE KEY	
Encrypted, and the password is:	
Cancel	Save

💊 注意:確保為要使用ZTNA訪問的每個應用程式新增所有證書。

為此示例配置的應用程式設定如下:

應用程式1:測試FMC Web UI(應用程式組1的成員)

	Enable	d
Application Settings		
Application Name*		
FINC		
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	E	
Pv4 NAT Source 👔		
Select V	F	
Application Group		
External_Duo X 🗸	_	
		١
SAML Service Provider (SP) Metadata		
SAMI Identity Provider (IdP) Metadata		
Shire dentity Provider (dP) metadata		
ke-Authentication interval		
Security Zones and Security Controls		

將應用程式新增到應用程式組1後,將繼承此應用程式的其餘設定。您仍然可以使用不同的設定覆蓋 安全區域和安全控制。

檢視已配置的應用程式,然後按一下Finish。

Add Application

			Enabl	ed 🌒
1	Application Settings			Edit
	Application Name External URL Application URL IPv4 NAT Source Application Certificate Application Group SAML Service Provider (SP) Metadata Configurations are derived from Application SAML Identity Provider (IdP) Metadata Configurations are derived from Application Re-Authentication Interval	FMC https://ao-fmc-ztna.cisco.local https://ao-fmc-ztna.cisco.local - ao-fmc-ztna.cisco.local External_Duo n Group 'External_Duo'		
	Security Zanas and Security Controls			Edit
3	Security Zones and Security Controls Security Zones Intrusion Policy Variable Set Malware and File Policy	Inherited: (Outside) Inherited: (None) Inherited: (None) Inherited: (None)		Edit
			Cancel	Finish

0 ×

應用程式2:CTB Web UI(應用程式組2的成員)

下面是此應用程式的配置摘要:

		Enabled
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	
SAML Service Provider (SP) Metad	ata	
Configurations are derived from App	lication Group 'Azure_apps'	
SAML Identity Provider (IdP) Metad	lata	
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	ols	Edit
Security Zones	Inherited: (Outside)	
Intrusion Policy	Inherited: (None)	
Variable Set	Inherited: (None)	
Malware and File Policy	Inherited: (None)	
		Cancel Finish

注意:請注意,對於此應用程式,網路對象「ZTNA_NAT_CTB」配置為IPv4 NAT源。通過此 配置,遠端使用者的源IP地址將轉換為已配置對象內的IP地址,然後再將資料包轉發到應用程 式。 進行此配置是因為應用程式(CTB)預設路由指向除安全防火牆之外的網關,因此返回流量未傳 送到遠端使用者。通過此NAT配置,已在應用上配置靜態路由,使子網ZTNA_NAT_CTB可以

通過安全防火牆訪問。

配置好應用程式後,它們現在顯示在相應的應用程式組下。

-	710											
ZINA	-TAG /											Targeted: 1 device
											Groups	3 Applications:
Ap	plications	Set	tings									
Bulk A	ctions	~	Q, Filter	by Name, IdP SAML missing, Enabled/Disabled						Add Application Gr	roup	Add Application
	Name			External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malwa	re and File Policy	Enabled	
~	Azure_apps (1	Applica	stion)			https://sts.v	. Outside (Inherited)	None (Inherited)	None	(Inherited)		*/*
	CTB			https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None	(Inherited)	True	*/*
~	External_Duo	(1 Appli	cation)			https://sso-	. Outside (Inherited)	None (Inherited)	None	(Inherited)		× / 1
	FMC			https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None	(Inherited)	True	2/1

最後,儲存更改並部署配置。

驗證

配置到位後,遠端使用者可以通過外部URL訪問應用程式,並且如果相應IdP允許他們訪問。

應用程式1

1.使用者開啟Web瀏覽器並導航到應用程式1的外部URL。在這種情況下,外部URL為「https://ao-fmc-ztna.cisco.local/」

✤ 注意:外部URL名稱必須解析為已配置的安全防火牆介面的IP地址。在本例中,它解析為外部 介面IP地址(192.0.2.254)

2.由於這是新訪問,因此使用者被重定向到為應用程式配置的IdP登入門戶。

$\leftarrow \rightarrow \mathbf{G}$	O A https://sso-		े 🔂	⊌ ⊜	ப்	≡
		ालांग दस्तर्ट Single Sign-On				
		al				
		Password				
		Log in				
		Secured by Duo				

3.向使用者傳送Push for MFA(這取決於IdP上配置的MFA方法)。





Are you logging in to External Applications ZTNA?





③ 1:13 p.m.



2.由於這是新訪問,因此使用者被重定向到為應用程式配置的IdP登入門戶。

← → C ill login.microsoftonline.com/		annanananananana k k 💷	Person Commission ()
	Microsoft		
	Sign in		
	a factoria con		
	Can't access your account?		
	Next		
	Sign-in options		
← → C ≤ Iogin.microsottonline.com/login.srf			
← → C			
← → C 单 login.microsoftonline.com/login.srf			
← → C é login.microsoftonline.com/login.srf			
← → C é login.microsoftonline.com/login.srf			
← → C a login.microsoftonline.com/login.srf			
← → C			
← → C ▲ login.microsoftonline.com/login.srf			
← → C ▲ 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 ■ login.microsoftonline.com/login.srf	Microsoft		
← → C a login.microsoftonline.com/login.srf	Microsoft		
	Microsoft Approve sign in request		
← → C a login.microsoftonline.com/login.srf	Microsoft Approve sign in request Open your Authenticator app, and enter the number shown to sign in.		
	Microsoft Microsoft Approve sign in request unber shown to sign in.		
 Iogin.microsoftonline.com/login.srf 	Microsoft Microsoft Approve sign in request Open your Authenticator app, and enter the number shown to sign in. 67		
 C Iogin.microsoftonline.com/login.srf 	Microsoft Dependent of a general to a gener		
 C Iogin.microsoftonline.com/login.srf 	Microsoft Microsoft Microsoft Moreo Sign in cequest Moreo Authenticator app, and enter the number shown to sign in. Moreo Marcolater app.		
 C Iogin.microsoftonline.com/login.srf 	 Microsoft Microsoft Deprove sign in equest number shown to sign in. Open your Authenticator app, and enter the number shown to sign in. Open your Authenticator app, and enter the number shown to sign in. 		
	 Microsoft Denyour Authenticator app, and enter the number shown to sign in. On your Authenticator app, and enter the number shown to sign in. On your Authenticator app, and enter the number shown to sign in. 		
C a login.microsoftonline.com/login.srf	 Microsoft Microsoft Open your Authenticator app, and enter the number shown to sign in. On your Authenticator app, and enter the number shown to sign in. On your Authenticator app, and enter the number shown to sign in. Other app of the sum of the sum		
C Inglin.microsoftonline.com/login.srf	<text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text>		
C A login.microsoftonline.com/login.srf	<text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text>		
C Iogin.microsoftonline.com/login.srf	<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></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></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><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></section-header></section-header>		

3.向使用者傳送Push for MFA(這取決於IdP上配置的MFA方法)。







關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。