为FMC管理访问配置双因素身份验证

目录

 箇介

 先决条件

 要求

 費求

 使用的组件

 背景信息

 身份验证流程

 身份验证流程说明

 配置

 「MC的配置步骤

 」5E的配置步骤

 」0u會理门户的配置步骤

 数障排除

 相关信息

简介

本文档介绍在Firepower管理中心(FMC)上为管理访问配置外部双因素身份验证所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题:

- Firepower管理中心(FMC)对象配置
- 身份服务引擎(ISE)管理

使用的组件

- 运行版本6.3.0的思科Firepower管理中心(FMC)
- 运行版本2.6.0.156的思科身份服务引擎(ISE)
- 支持版本的Windows(<u>https://duo.com/docs/authproxy-reference#new-proxy-install</u>),可连接 到FMC、ISE和Internet以充当Duo身份验证代理服务器
- 访问FMC、ISE和Duo管理门户的Windows计算机
- Duo Web帐户

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

FMC管理员根据ISE服务器进行身份验证,Duo Authentication Proxy服务器将向管理员的移动设备 发送推送通知形式的附加身份验证。

身份验证流程



身份验证流程说明

- 1. 向Cisco FMC发起主要身份验证。
- 2. 思科FMC向双身份验证代理发送身份验证请求。
- 3. 主要身份验证必须使用Active Directory或RADIUS。
- 4. Duo Authentication Proxy connection established to Duo Security over TCP端口443。
- 5. 通过Duo Security的服务进行辅助身份验证。
- 6. Duo身份验证代理收到身份验证响应。
- 7. 思科FMC GUI访问权限已授予。

配置

要完成配置,请考虑以下部分:

FMC的配置步骤

步骤1:导航到System > Users > External Authentication。 创建外部身份验证对象并将身份验证方

Subscription State Sta

Overview Analysis Policies Devices	Objects AMP Intellig	ence						Deploy	🕘 🔍 Sy	stem Help 🔻	admin 🔻
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health 🔻	Monitoring •	Tools •
Users User Roles External Author	entication										
	External Authenticatio Authentication Method Name * Description Primary Server Host Name/IP Address * Port *	n Object RADIUS 😨 DuoAuthProxy 10.106.44.177 1812		ex. Ii	P or hostname						
	RADIUS Secret Key	•••••									
	Backup Server (Option	nal)									
	Host Name/IP Address Port RADIUS Secret Key	1812		ex. Il	P or hostname						
	RADIUS-Specific Parar	meters									
	Timeout (Seconds) Retries Access Admin Administrator	30 3									

单击Save和Apply。忽略如图所示的警告:

Overview Ana	sis Policie	s Devices	Objects	AMP	Intelligence							Deplo	y 🧕	System He	lp • admin •
							Configuration	Users	Domains	Integration	Updates	Licenses *	Health	 Monitor 	ing • Tools •
						One or more en don't have defin	abled external auther red user roles.	ntication obje	cts						
Users User R	es Extern	al Authentic	ation												
													😑 Save	🔀 Cancel	Save and Apply
Default User Role: N	ie	:	Shell Authentic	ation	Disabled	0							•	Add External Au	thentication Object
Name													Meth	od Enab	led
1. DuoAuthProxy													RADI	JS 📿	26

第二步: 导航到System > Users > Users。 创建用户,然后检查身份验证方法作为外部,如图所示 :

User Configuration							
User Name	cpiplani						
Authentication	Use External Authentication Method						
Options	Exempt from Browser Session Timeout						
User Role Configuration							
Default User Roles	 Administrator External Database User Security Analyst Security Analyst (Read Only) Security Approver Intrusion Admin Access Admin Access Admin Network Admin Maintenance User Discovery Admin Threat Intelligence Director (TID) User 						

步骤1:下载并安装Duo身份验证代理服务器。

登录到Windows计算机并安装Duo Authentication Proxy Server

建议使用至少具有1个CPU、200 MB磁盘空间和4 GB RAM的系统

Selection Sele

第二步:配置authproxy.cfg文件。

在文本编辑器(如记事本++或写字板)中打开此文件。

◆ 注意:默认位置位于C:\Program Files(x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

编辑authproxy.cfg文件并添加以下配置:

<#root>

[radius_client]

host=10.197.223.23

Sample IP Address of the ISE server

secret=cisco

Password configured on the ISE server in order to register the network device

FMC的IP地址必须与RADIUS密钥一起配置。

<#root>

radius_ip_1=10.197.223.76

IP of FMC

radius_secret_1=cisco

Radius secret key used on the FMC

failmode=safe
client=radius_client
port=1812
api_timeout=

确保配置ikey、skey和api_host参数。要获取这些值,请登录您的双核帐户(<u>Duo Admin Login)</u>并导 航到应用>保护应用。接下来,选择RADIUS身份验证应用,如图所示:

RADIUS

See the RADIUS documentation II to integrate Duo into your RADIUS-enabled platform.

Details



集成密钥= ikey

secret key = skey

API主机名= api_host

第三步:重新启动Duo Security Authentication Proxy服务。保存文件并重新启动Windows计算机上的Duo服务。

打开Windows服务控制台(services.msc)。在服务列表中找到Duo Security Authentication Proxy Service,然后单击Restart,如图所示:

			Services				- 0
File Action View Het	*						
H 🕂 📷 🖾 🗟 🖨	1 m + + + + + + + + + + + + + + + + + +						
Sevies (and)	Services (Local)						
Our Ser	Security Authoritization Provy vice	Name * G.DCOM Saver Process Lauture	Description. The DCOMLADNON set	Status Rensing	Startup Type Automatic	Log-On As Local System	
20mg	the service of the service	Onice Association Service Onice Install Service Onice Install Service	Enables pairing between. Enables a computer to		Manual (Trigger Stat) Manual (Trigger Stat) Manual (Trigger Stat)	Local System Local System Local System	
		Q.073 Namespace Q.075 Replication	Enables yes to group s Enables yes to synchro	Running Running	Automatic Automatic	Local System Local System	
		Q, DHCP Clark Q, DHCP Sever Q, Diagnostic Policy Service	Repoten and updates I., Performs 307/IP confi., The Disprostic Policy S.,	Running Running	Automatic Automatic Automatic Delayed	Local Service Network Service Local Service	
		Q, Diagnostic Service Heat Q, Diagnostic System Heat	The Disgnostic Service The Disgnostic System		Manual Manual	Local Service Local System	
		Displaying tensors Displaying Line Tracking Cl. Distributed Line Tracking Cl. Distributed Tracket Tracking Cl.	Maintains Into Behnes	Ranning	Automatic Manual Automatic Dalacent	Local System Local System Network Service	
		Q, DNS Clant Q, DNS Server	The DNS Client service - Evables (INS clients to c.,	Running Running	Automatic (Trigger S., Automatic	Network Service Local System	
		C. Di Rate Server	This service hosts the D		Manual	Local System	
		C. Encrypting File System (EV) Extensible Authentication F	Provides the core file a The Edwards's Authentia		Manual (Trigger Start) Manual	Local System Local System	
		Q. File Replication Q. FileDilla Server FTP server	Synchronizes folders mi	Renning.	Disabled Automatic	Local System Local System	

ISE的配置步骤

步骤1:导航到Administration > Network Devices,单击Add以配置网络设备,如图所示:

♦ 注意:10.106.44.177是Duo身份验证代理服务器的示例IP地址。

duale Identity Services Engine	Home	Operations F	Policy - Admi	nistration V	ork Centers	
System Identity Management	Network Resources Device	Portal Management	pxGrid Services	Feed Service	Threat Centric N	AC
✓ Network Devices Network Device C	Groups Network Device Profiles	External RADIUS Ser	vers RADIUS S	Server Sequences	NAC Managers	External MDM
C Natural Daviasa	Network Devices List > DuoAut	hproxy				
Network Devices	Network Devices					
	* Name	DuoAuthproxy				
Device Security Settings	Description					
	IP Address *	IP : 10.106.44.177			/ 32	
	* Device Profile	就 Cisco 👻 🕀				
	Model Name	.				
	Software Version					

按照authproxy.cfg中所述配置secret中的共享密钥,如图所示:

dentity Services Engine	Home	Context Visibility Operations Policy Administration Work Centers
System Identity Management	- Network	Resources
Network Devices Network Device 0	Groups	etwork Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM
0		
Network Devices	\checkmark	
Default Device		
Device Security Settings		RADIUS UDP Settings
		Protocol RADIUS
		* Shared Secret Show
		Use Second Shared Secret 🔲 🕡
		Show
		CoA Port 1700 Set To Default

第二步:导航到管理>身份。 单击Add以配置身份用户,如图所示:

• System • Identity Management • Network Resources • Device Portal Management pxGrid Services • Feed Service • Threat Centric NAC • Identities Groups External Identity Sources Identity Source Sequences • Settings Users • Network Access User • Network Access User Latest Manual Network Scan Results • Network Access User • Name cipilani Status • Enabled • • Passwords • Password • Login Password • • • • • • • • • • • • • • • • • • •	dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
✓ Identities Groups External Identity Sources Identity Sources Sequences > Settings Users Users Latest Manual Network Scan Results ✓ Network Access Users ✓ Network Access User ✓ Name [pipIani ✓ Status ✓ Enabled ● Email ✓ Passwords Password Type: Internal Users Password Login Password Login Password Concrate Password		Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Users Network Access Users List > cpiplani I Latest Manual Network Scan Results Name cpiplani Status Enabled Fasswords Password Type: Internal Users Password Re-Enter Password Concrate Password () 	✓ Identities Groups External Ident	ity Sources Identity Source Sequences
Password Ke-Enter Password Generate Password Generate Password Generate Password Generate Password	Users Latest Manual Network Scan Results	Network Access Users List > cpiplani Network Access User Name cpiplani Status Cenabled Email Passwords Passwords Password Type: Internal Users
Eliquid Edgawold		* Login Password Generate Password ()

Duo管理门户的配置步骤

步骤1:创建用户名并在终端设备上激活Duo Mobile。

将该用户添加到双核云管理网页上。 导航到Users > Add users,如图所示:



♦ 注意:确保最终用户安装了Duo应用。

<u>手动安装IOS设备Duo应用程序</u>

手动安装适用于Android设备的Duo应用程序

第二步:代码的自动生成。

添加用户的电话号码,如图所示:

Phones

Add Phone You may reamange the phones by dragging and dropping in the table. This user has no phones. Add one.



选择Activate Duo Mobile,如图所示:

Device Info		
Not using Duo Mobile Activate Duo Mobile	Model Unknown	OS Generic Smartphone

选择Generate Duo Mobile Activation Code,如图所示:

Deshlocend	Determined 2 these levels (instates 2 Active Lee Matrix Activate Duro Mobile								
Policies									
Applications	Hourace B	Activate buy mobile							
Users	This form allows you to penerate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to penerate passcodes on their mobile device or a directivity of Duo Bush.								
27A Devices	Note: Cenerating an act	Note: Conserving an activation code will invalidate any existing from Mattile contentiate for this device will it is activated with the new activation code.							
Phones									
Hardware Tokana	Prote	Generic Smartphone							
den en									
or or other	Francisco	the local star second							
Administrations	Coper prices	And house and here an							
Reports									
Settings		Generate Due Mobile Activitien Code							

选择Send Instructions by SMS,如图所示:

Deshboard	Castinged 3 Prices Securit Structures 3 Autom Duciments								
Pulcies	Activate Duo Mobile								
Applications	Activate Duo Nicolie								
Uses	A new Quo Mobile activation activation indiscriments in the	A new Quo Muble activation code has been parented, and any old oredentials have been invalidated. You now have the option to deliver the installation instructions and/or access to the first							
25A Devices									
Phone Rectore Totace	Plane	Generic Smarphone							
MOUNT & UP	Installation instructions	Send installation instructions via SMS							
Groups		Viteloome to Duct Please install Duc-Mobile from your app							
Becorts		store.							
Settings		A.							
Dilling									
Region) Elegende your plat for expect. Account 10	Activation instructions	Send activation instructions via SMS To activate the app, tap and open this link with Ouo Mobile:							
Instant 0		×							
Regular Comes Reconstruction of Deer Guide of		Send Instructions by SNIS or skip this step							

单击SMS中的链接,Duo应用将链接到"设备信息"部分中的用户帐户,如图所示:

Dashboard Policies Applications Users Users 25A Devices Ponse Ponse Nethener Stans medurin & Lotif Groups Administrators Reports Settings Device Info Settings Device Info Settings					
Policies Applications Users 25A Devices Prones Prones Prones Medeum Stans medulin & Loff Groups Administrators Reports Settings Using Duo Mobile 3.29.0 Reactivate Duo Mobile 3.29.0 Reactivate Duo Mobile 3.29.0 Settings Model Image: Device Info	Dashboard	Dashboard >	Phones > Phone:		
Applications Users 25A Devices Prones Nerdware Totans WebAren & Udf Groups Administrators Reports Settings Using Duo Mobile 3.29.0 Cases 1 hour ago Medel Medel Of Settings	Policies				
Users SFA Devices Phones Nachware Tokers Webhare & Lubi Groups Administrators Reports Settings Using Duo Mobile 3.29.0 Nachware Duo Mobile 3.29.0 Reports Settings Last Seen Thom ago	Applications				
SFA Devices Authentication devices Proves Authentication devices Nethease Tokens Construction WebAuter & UDF Device Info Administrators Using Duo Mobile 3.29.0 Reports Using Duo Mobile 3.29.0 Settings Construction devices	Users		cpiplani (Chakahu Piplani)	Å, Attach a user	
Prones can share multiple users Hardware Tokens users WebAutre & UDF Device Info Administrators Using Due Mobile 3.29.0 Reports Os Settings Using Due Mobile 3.29.0 Income Source Medel	2FA Devices	2		Authentication devices	
Hardware Tokens WebAutre & UDF Groups Administrators Reports Settings Using Duo Mobile 3.29.0 Reactivate Duo Mobile 3.29	Phones			can share multiple	
WebAutrin & LOP Groups Device Info Administrators Reports Settings	Hardware Tokens			users	
Groups Device Info Administrators Image: Construction of the state of the sta	WebAuthin & UDF				
Administrators Reports Settings Using Due Mobile 3.29.0 Reactivate Due Mobile C Last Seen Theor age	Groups	Device In	nfo		
Reports Settings Construction Control	Administrators		Union Paus Mobile 3 28 A	- Mindred	M
Settings O Last Seen 1 hour apo	Reports	240	Reactivate Duo Mobile	([])	(🖨) Android 9
	Settings		O Last Seen 1 hour ago		

验证

使用本部分可确认配置能否正常运行。

使用在ISE用户身份页面添加的用户凭证登录到FMC。您必须在您的终端上收到双因素身份验证 (2FA)的双重PUSH通知,请批准该通知,然后FMC将按如下图所示登录:

Login Request



CISCO SYSTEMS



August 2, 2019, 7:37 PM





关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。