Configuration de l'authentification à deux facteurs Duo pour l'accès à la gestion FMC

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Flux d'authentification Flux d'authentification expliqué Configurer Étapes de configuration sur FMC Étapes de configuration sur ISE Étapes de configuration sur le portail Duo Administration Vérifier Dépannage Informations connexes

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs externe pour l'accès à la gestion sur Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'objets Firepower Management Center (FMC)
- Administration ISE (Identity Services Engine)

Composants utilisés

- Cisco Firepower Management Center (FMC) version 6.3.0
- Cisco Identity Services Engine (ISE) exécutant la version 2.6.0.156
- Version prise en charge de Windows (<u>https://duo.com/docs/authproxy-reference#new-proxy-install</u>) avec connectivité à FMC, ISE et Internet pour servir de serveur proxy d'authentification Duo
- Machine Windows afin d'accéder à FMC, ISE et Duo Administration Portal
- Compte Web Duo

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€TMincidence possible des commandes.

Informations générales

L'administrateur FMC s'authentifie auprès du serveur ISE et une authentification supplémentaire sous la forme d'une notification de transmission est envoyée par le serveur proxy d'authentification duo au périphérique mobile de l'administrateur.

Flux d'authentification



Flux d'authentification expliqué

- 1. Authentification principale initiée vers Cisco FMC.
- 2. Cisco FMC envoie une demande dâ€[™]authentification au proxy dâ€[™]authentification duo.
- 3. L'authentification principale doit utiliser Active Directory ou RADIUS.
- 4. Connexion proxy d'authentification duo établie avec Duo Security sur le port TCP 443.
- 5. Authentification secondaire via le service de Duo Security.
- 6. Le proxy d'authentification duo reçoit la réponse d'authentification.
- 7. L'accès à l'interface utilisateur graphique Cisco FMC est autorisé.

Configurer

Pour terminer la configuration, tenez compte des sections suivantes :

Étapes de configuration sur FMC

Étape 1. Accédez à System > Users > External Authentication. Créez un objet d'authentification externe et définissez la méthode d'authentification sur RADIUS. Assurez-vous que l'administrateur est sélectionné sous Rôle d'utilisateur par défaut, comme indiqué dans l'image :

			Configuration	Users	Domains	Integration	Update
			g				
Users User Roles External Au	uthentication						
	External Authenticatio	on Object					
	Authentication Method	RADIUS 😋					
	Name •	DuoAuthProxy					
	Description						
	Primary Server						
	Host Name/IP Address *	10.106.44.177		ex.	IP or hostname		
	Port *	1812					
	RADIUS Secret Key	•••••					
	Backup Server (Option	nal)					
	Host Name/IP Address			ev.	IP or hostname		
	Port	1812		-			
	RADIUS Secret Key						
	RADIUS-Specific Para	meters					
	Timeout (Seconds)	30					
	Retries	3					
	Access Admin						
	Administrator						
	Conveiler Applyint						
	Security Analyst						
	Security Analyst (Read Only)						
	Security Approver						
	Threat Intelligence Director						
	(110) 0361	Access Admin					
	Default User Role	Administrator Discovery Admin		To s	pecify the defaul	It user role if user	r is not fou
		External Database User		uny	group		
	Shell Access Filter						
	Administrator Shell Access						
	User List 0			ex. (user1, user2, us	er3	
	(Mandatory for FTD devices)						
	Define Custom RADI	US Attributes					
	Additional Test Param	eters					
	User Name						
	Password						
	*Required Field						
		Save Test Can	icel				

Remarque : 10.106.44.177 est l'exemple d'adresse IP du serveur proxy d'authentification duo.

Cliquez sur **Enregistrer** et **appliquer**. Ignorez l'avertissement comme indiqué dans l'image :

Overvie	w Analysis	Policies	Devices	Objects	AMP	Intelligence							
								Configuration	Users	Domains	Integration	Updates	Lice
							One or more ena don't have define	bled external authe ed user roles.	ntication obje	octs			
Users	User Roles	External	Authentic	ation									
Default Use	r Role: None		:	Shell Authe	ntication	Disabled	0						
Name													
1. DuoAu	thProxy												

Étape 2. Accédez à Système > Utilisateurs > Utilisateurs. Créez un utilisateur et cochez la case Authentication Method as External (Méthode d'authentification externe), comme indiqué dans l'image :

User Configura	ition
User Name	cpiplani
Authentication	Use External Authentication Method
Options	Exempt from Browser Session Timeout
User Role Conf	figuration
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 Save

Étape 1. Téléchargez et installez Duo Authentication Proxy Server.

Connectez-vous à l'ordinateur Windows et installez le serveur proxy d'authentification Duo

Il est recommandé d'utiliser un système avec au moins 1 processeur, 200 Mo d'espace disque et 4 Go de RAM

Remarque : cette machine doit avoir accès à FMC, au serveur RADIUS (ISE dans notre cas) et au cloud Duo (Internet)

Ouvrez ce fichier dans un éditeur de texte tel que Bloc-notes++ ou WordPad.

 $Remarque: l'emplacement par défaut se trouve à l'adresse C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg$

Modifiez le fichier authproxy.cfg et ajoutez cette configuration :

<#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

L'adresse IP du FMC doit être configurée avec la clé secrète RADIUS.

<#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=

Assurez-vous de configurer les paramètres ikey, skey et api_host. Afin d'obtenir ces valeurs, connectez-vous à votre compte Duo (<u>Connexion Admin Duo</u>) et naviguez vers **Applications > Protect an Application**. Sélectionnez ensuite l'application d'authentification RADIUS comme indiqué dans l'image :

RADIUS

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

Details

Integration key		select
Secret key	Click to view.	select
	Don't write down your secret key or share it with a	nyone.
API hostname		select

Clé d'intégration = ikey

clé secrète = skey

Nom d'hôte API = api_host

Étape 3. Redémarrez le service proxy d'authentification de sécurité duo. Enregistrez le fichier et redémarrez le service Duo sur l'ordinateur Windows.

Ouvrez la console des services Windows (services.msc). Recherchez **Duo Security Authentication Proxy Service** dans la liste des services, puis cliquez sur **Restart** comme indiqué dans l'image :

			Services				_ 0 X
lie Action Ves	Thep						
++ 📰 🖂 (4 🖬 🖬 💷 🕨 🖬 🖬 🖬 🖬						
Sevice (Loot)	Services (Local)						
	Duo Security Authentication Prosy	Name	Description	Setup	Statup Type	Log On As	
	Service	Q, DCOM Server Process Laun	The DOOMLADNOH se-	Running	Automatic	Local System	
		C. Device Association Service	Enables pairing between.		Manual (Tripper Start)	Local System	
	200 the service	C Device Install Service	Enables a computer to		Manual (Trigger Start)	Local System	
	SALES IN BOUCH	C. Device Setup Manager	Enables the detection,		Manual (Trigger Start)	Local System	
		Q, DPS Namespece	Enables you to proup s	Running	Automatic	Local System	
		Q.0FS Replication	Enables you to synchro	Running	Automatic	Local System	
		G, DHCP Clant	Registers and updates I	Running	Automatic	Local Service	
		G, DHCP Server	Performs TCR/IP confi	Running	Automatic	Network Service	
		C, Diagnostic Policy Service	The Diagnostic Policy S	Running	Automatic Delayed	Local Service	
		C Diagnestic Service Heat	The Diagnostic Service		Manual	Local Service	
		C. Diagnostic System Host	The Disgnostic System		Manual	Local System	
		C. Diagnostics Tracking Service	The Diagnostics Tracki	Running	Automatic	Local System	
		C, Dutributed Link Tracking CL.	Maintains Into Into-		Manual	Local System	
		C Distributed Transaction Co	Coordinates transaction	Running	Automatic Delayed	Network Service	
		Q. (INS Clent	The DAS Client service	Running	Automatic (Trigger S.,	Network Service	
		G, 0NS Server	Enables (192) clients to c	Running	Automatic	Local System	
		Q, D1 Role Server	This service hosts the D		Manual	Local System	
		Q Due Security Buthentication				Local System	
		C. Encrypting File System (DFS)	Provides the core file e		Manual (Trigger Start)	Local System	
		C. Educible Authentication P	The Extensible Authenti		Manual	Local System	
		Q. File Replication	Synchronizes folders wi		Disabiled	Local System	
		Child Server FTP server		Running	Automatic	Local System	

Étapes de configuration sur ISE

Étape 1. Accédez à Administration > Network Devices, cliquez sur Add afin de configurer le périphérique réseau comme indiqué dans l'image :

dentity Services Engine	Home	isibility > Operations	► Policy
System Identity Management	- Network Resources	Device Portal Management	pxGrid Services Feed Se
▼ Network Devices Network Device G	Groups Network Device	Profiles External RADIUS	Servers RADIUS Server Sequ
Network Devices Default Device Device Security Settings	Network Devices List Network Devices	> DuoAuthproxy * Name DuoAuthproxy escription * IP : 10.106.44.17 ce Profile Cisco Getting del Name Getting	 77
	Softwar	e Version]

Configurez le **secret partagé** comme indiqué dans le fichier **authproxy.cfg** dans le fichier **secret** comme indiqué dans l'image :

cisco Iden	tity Serv	ices Engine	Home	Context	Visibility	 Operations 	Policy	▼ Adn	ninistration
 System 	 Identi 	ty Management	✓ Networ	rk Resources	Device	Portal Management	pxGrid S	Services	Feed Ser
- Network	Devices	Network Device	Groups	Network Device	ce Profiles	External RADIUS	Servers	RADIUS	Server Seque
			3						
Network Devi	ces		\checkmark	▼ RADIUS A	Authenticatio	n Settings			
Default Devic	e								
Device Secur	ity Setting	S		RADIUS	UDP Setting	gs			
							Pr	rotocol	RADIUS
							* Shared	Secret	•••••
						Use Seco	ond Shared	Secret [i
							Co	A Port	1700

Étape 2. Accédez à Administration > Identities. Cliquez sur Add afin de configurer l'utilisateur Identity

Remarque : 10.106.44.177 est l'exemple d'adresse IP du serveur proxy d'authentification duo.

comme indiqué dans l'image :

dentity Services Engine	Home	Context Visibility	 Operations 	▶ Policy	✓ Administration
► System	Network R	esources	ce Portal Managemen	t pxGrid	Services Feed Services
✓ Identities Groups External Ide	entity Sources	Identity Source Se	quences > Setting	s	
	O Network /		cninlani		
Users	Network 7	ACCESS USERS LIST >	cpipiani		
Latest Manual Network Scan Results	▼ Net	work Access Use	5 7		
	* Nam	e cpiplani			
	Statu	is 🔽 Enabled	•		
	Ema	ail			
	▼ Pa	sswords			
	Pass	sword Type: Int	ernal Users	Ŧ	
		Pass	sword		Re-Enter Password
	* Log	gin Password •••			•••••
	Enat	ble Password			

Étapes de configuration sur le portail Duo Administration

Étape 1. Créez un nom d'utilisateur et activez Duo Mobile sur le périphérique final.

Ajoutez l'utilisateur sur la page Web d'administration du cloud Duo. Accédez à **Users > Add users** comme indiqué dans l'image :

DU O	9. Search for users, gro	ups, applications, or devices
Dashboard Policies	Add User	dd User
Applications Users Add User	Adding Users Most applications allo Learn more about add	ow users to enroll themselves after they complete primary authentication. ding users Cf
Pending Envollments Bulk Enroll Users Import Users Directory Sync Bypass Codes	Username	opiplani Should match the primary authentication username.
2FA Devices Groups Administrators		Add User

Remarque : vérifiez que l'application Duo est installée sur l'utilisateur final.

Installation manuelle de l'application Duo pour les périphériques IOS

Installation manuelle de l'application Duo pour les appareils Android

Étape 2. Génération automatique de code.

Ajoutez le numéro de téléphone de l'utilisateur comme illustré dans l'image :

Phones Visu may reamings the phones by dragging and dropping in the table. Add Phone							
	This user has no phones. Add one.						
Due	9. Search for users, gr	oups, applications, or devices					
Dashboard	Dashboard > Users > 1	piplani > Add Phone					
Policies	Add Bhon	2					
Applications	Add Phon	e					
Users	Type	Phone					
Add User		 Tablet 					
Pending Envolments							
Buk Ervol Users	Phone number	+1 201-555-5555 Show extension field					
Import Users							
Bypass Codes		Add Phone					
2FA Devices							

Choisissez Activate Duo Mobile comme indiqué dans l'image :



Choisissez Generate Duo Mobile Activation Code comme indiqué dans l'image :

Destitioard	Antipart 3 Reservants	Terretory & Annual Terretory				
Policies	Activate Du	o Mobile				
Applications	Activate Du	O MODILE				
Users	This form allows you to per- mobile device or authentics	This form allows you to parentle a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to panentle passocides on their mobile design on the application of the the set of the set of the set of the set of the the set of the set				
2FA Devices	Note for any set of the					
Protest	NOR GROUPING IN SCHOOL	Note: Generating an activation code will invandance any existing Duo Motore prependers for this device until it is activated with the new activation code.				
Hardware Tokana						
Westame & LOF	Phote	Generic Smartphone				
Groups						
Administrations	Expiration	24 hours after generation				
Reports						
Settings		Generate Dus Mobile Activation Code				

Choisissez Send Instructions by SMS comme indiqué dans l'image :

Deshlored Pulicies Applications Users	Activate Du Activate Du	Characterize 3 Antone Dax Index IO MObile on code has been generated, and any old oredentate have been invalidated. You now have the option to deliver the installation instructions and/or to user by SMS.
29A Devices Proves Turbuse Totans	Plane	Garent Smartphone
Oringes Administrations	Installation instructions	Send initializion instructions via IMB Velocome to Duci Please instal Duc Mobile from your app store.
Settings Billing		4
Report Liggeds your plan for mapport. Account D	Activation instructions	Bend activation instructions via BMS. To activate the app, top and sport this link with Oue Mobile:
Projekt Unite Reliable Unite Description (7 Unite Description (7		A feed trebuctions by SMI ar using this stop

Cliquez sur le lien dans le SMS, et l'application Duo est liée au compte d'utilisateur dans la section Device Info, comme le montre l'image :

Dashboard Policies Applications	Dashboard > Phones > Phone	•	
Users	cpiplani (Chakahu Piplani)	A Attach a user	
2FA Devices Phones Hardware Tokens		Authentication devices can share multiple users	
Weblann & LOF Groups	Device Info		
Administrators Reports Settings	Using Duo Mobile 3.29.0 Reactivate Duo Mobile © Lest Seen 1 hour ago	Medel	OS Android 9

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Connectez-vous au FMC à l'aide de vos identifiants d'utilisateur qui ont été ajoutés sur la page d'identité de l'utilisateur ISE. Vous devez obtenir une notification PUSH Duo sur votre terminal pour l'authentification à deux facteurs (2FA), l'approuver et FMC se connecterait comme indiqué dans l'image :



Sur le serveur ISE, accédez à **Operations > RADIUS > Live Logs**. Recherchez le nom d'utilisateur utilisé pour l'authentification sur FMC et sélectionnez le rapport d'authentification détaillé sous la colonne Détail. Dans cette section, vous devez vérifier si l'authentification a réussi, comme indiqué dans l'image :

In Identity Services Engine			
Overview		Steps	
Event	5200 Authentication succeeded	11001	Received RADIUS Access-Request
		11017	RADIUS created a new session
Username	cpiplani	11117	Generated a new session ID
Endpoint Id		15049	Evaluating Policy Group
		15008	Evaluating Service Selection Policy
Endpoint Profile		15041	Evaluating Identity Policy
Authentication Policy	Default >> Default	15048	Queried PIP - Normalised Radius.RadiusFl
Authorization Policy	Default >> Resin Authentinated Anness	22072	Selected identity source sequence - All_Us
Autorization Policy	Detaul Dasic_Nullenikaieu_Nucess	15013	Selected Identity Source - Internal Users
Authorization Result	PermitAccess	24210	Looking up User in Internal Users IDStore
		24212	Found User in Internal Users IDStore
		22037	Authentication Passed
			Evaluating Authorization Policy
Authentication Details	uthentication Details		Queried PIP - Radius.NAS-Port-Type
Source Timestamp	2019-07-11 03:50:38.694	15048	Queried PIP - Network Access.UserName
		15048	Queried PIP - IdentityGroup.Name
Received Timestamp	2019-07-11 03:50:38.694	15048	Queried PIP - EndPoints.LogicalProfile
Policy Server	ROHAN-ISE	15048	Queried PIP - Network Access.Authenticati
		15016	Selected Authorization Profile - PermitAcce
Event	5200 Authentication succeeded	22081	Max sessions policy passed
Username	cpiplani	22080	New accounting session created in Session
User Type	User	11002	Returned RADIUS Access-Accept

Authentication Identity Store Internal Users

Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

• Vérifiez les débogages sur Duo Authentication Proxy Server. Les journaux se trouvent à l'emplacement suivant :

C:\Program Fichiers (x86)\Duo Security Authentication Proxy\log

Ouvrez le fichier **authproxy.log** dans un éditeur de texte tel que Notepad++ ou WordPad.

Enregistre les extraits de journal lorsque des informations d'identification incorrectes sont saisies et que l'authentification est rejetée par le serveur ISE.

<#root>

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

10.197.223.76 is the IP of the FMC

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524) 2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):

login attempt for username u'cpiplani'

2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2 2019-08-04T18:54:17+0530 [RadiusClient (UDP)]

Got response

for id 199 from ('

10.197.223.23

', 1812);

code 3 10.197.223.23 is the IP of the ISE Server.

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials rejecter 2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):

Returning response code 3: AccessReject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response

• Sur ISE, accédez à **Operations** > **RADIUS** > **Live Logs** pour vérifier les détails de l'authentification.

Consignez les extraits d'authentification réussie avec ISE et Duo :

<#root>

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto 2019-08-04T18:56:16+0530 2019-08-04T18:56:16+0530 2019-08-04T18:56:16+0530 2019-08-04T18:56:16+0530	[DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34099 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for usern [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.2 [RadiusClient (UDP)] Got response for id 137 from ('			
10.197.223.23				
', 1812);				
code 2	<<<< At this point we have got successful authentication from ISE Server.			
2019-08-04T18:56:16+0530 2019-08-04T18:56:16+0530 2019-08-04T18:56:17+0530 2019-08-04T18:56:17+0530 2019-08-04T18:56:17+0530 2019-08-04T18:56:17+0530 2019-08-04T18:56:30+0530	<pre>[RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest [duoauthproxy.lib.httpDuoHTTPClientFactory#info] Starting factory <_DuoHTTPC] [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): 0 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26 [duoauthproxy.lib.httpDuoHTTPClientFactory#info] Starting factory <_DuoHTTPC] [duoauthproxy.lib.httpDuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC] [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):</pre>			
Duo authentication returned 'allow': 'Success. Logging you in				
1				
2019-08-04T18:56:30+0530	[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):			
Returning response code 2	: AccessAccept <<<< At this point, user has hit the approve button			
2019-08-04T18:56:30+0530 2019-08-04T18:56:30+0530	[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): 5 [duoauthproxy.lib.httpDuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC]			

Informations connexes

- <u>Authentification VPN RA utilisant Duo</u>
- Assistance et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.