# Configuración de la autenticación activa de FDM (portal cautivo)

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Diagrama de la red Configurar Verificación Troubleshoot

## Introducción

Este documento describe un ejemplo de configuración para Firepower Device Manager (FDM) con integración de Active Authentication (Captive-Portal). Esta configuración utiliza Active Directory (AD) como el origen y los certificados autofirmados.

## Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Certificados autofirmados.
- Secure Socket Layer (SSL)

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software:'

- Firepower Threat Defense 6.6.4
- Active Directory
- prueba de PC

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

#### Establecer identidad de usuario mediante autenticación activa

La autenticación es el acto de confirma la identidad de un usuario. Con la autenticación activa, cuando un flujo de tráfico HTTP proviene de una dirección IP para la que el sistema no tiene asignación de identidad de usuario, puede decidir si autenticar al usuario que inició el flujo de tráfico en el directorio configurado para el sistema. Si el usuario se autentica correctamente, se considera que la dirección IP tiene la identidad del usuario autenticado.

Si no se realiza la autenticación, no se impide el acceso a la red del usuario. En última instancia, las reglas de acceso deciden qué acceso se debe proporcionar a estos usuarios.

#### Diagrama de la red



## Configurar

#### Implementar la política de identidad

Para habilitar la adquisición de identidad del usuario, de modo que se conozca al usuario asociado a una dirección IP, debe configurar varios elementos

Paso 1. Configurar el rango de identidad AD

Tanto si recopila la identidad del usuario de forma activa (solicitando la autenticación del usuario) como pasiva, debe configurar el servidor de Active Directory (AD) que tiene la información de identidad del usuario.

Navegue hasta **Objetos > Servicios de identidad** y seleccione la opción **AD** para agregar Active Directory.

CISCO. Firepower Device	e Manager Monitoring Policies	Objects Device: firepower	> @ ?	* admin * Administrator
Object Types ←	Identity Sources			
C Networks	2 objects		Q Search	+ ~
S Ports	* NAME	TIPE	VALUE	RADIUS Server
Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
Application Filters				AD
C <sup>9</sup> URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client Pro				
E Identity Sources				
1 Users				

Agregue la configuración de Active Directory:

Identity Realm is used for Identity Policies and Remote this realm.	e Access VPN. Any changes impact all features that use
Name	Туре
Active_Directory	Active Directory (AD)
Directory Username	Directory Password
Base DN	AD Primary Domain
CN=Users,DC=ren,DC=lab	ren.lab
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
172.17.4.32:389	<u>Test</u> 👻
Add another configuration	
	CANCEL

#### Paso 2. Crear certificados autofirmados

Para crear una configuración de Portal cautivo, necesita dos certificados uno para el portal cautivo y otro para el descifrado SSL.

Puede crear un certificado autofirmado como en este ejemplo.

Vaya a Objetos > Certificados

cisco. Firepower Devi	ce Manager Monitoring Policies Objects Device: firepower	S. 🖄 🗐 ? : admin Administrator
Object Types ←	Certificates	
C Networks	120 objects	Q Search + V
S Ports		Preset filters: System.defined - User.defined Add Internal CA
Security Zones	B NAME TYPE	Add Internal Certificate
Application Filters	1 NGFW-Default-InternalCA Internal CA	Add Trusted CA Certificate
<b>n0</b> 1101 n	2 ssl_captive_portal Internal CA	
OF URLS	3 DefaultInternalCertificate Internal Certificate	
Geolocations	4 DefaultWebserverCertificate Internal Certificate	

Certificado de firma automática del portal cautivo:

Add Internal Certificate	8 ×
Name	
captive_portal	
Country	State or Province
Mexico (MX)	Mexico
Locality or City	
Mexico	
Organization	Organizational Unit (Department)
MexSecTAC	MexSecTAC
Common Name	
fdmcaptive	
You must specify a Common Name to use the ce	rtificate with remote access VPN.
	CANCEL SAVE

Certificado con firma automática SSL:

## Add Internal CA

Name		
ssl_captive_portal		
Country		State or Province
Mexico (MX)	~	Mexico
Locality or City		
Mexico		
Organization		Organizational Unit (Department)
MexSecTAC		MexSecTAC
Common Name		
ss_fdmcaptive		
You must specify a Common Name to use	the certi	ficate with remote access VPN.
		CANCEL SAVE

Paso 3. Crear regla de identidad

Navegue hasta **Políticas > Identidad >** seleccione el botón **[+]** para agregar una nueva regla de identidad.

Debe crear la política de identidad para configurar la autenticación activa, la política debe tener los siguientes elementos:

- Origen de identidad de AD: Lo mismo que agrega en el paso número 1
- Acción: AUTH ACTIVE
- Certificado de servidor: El mismo certificado autofirmado que creó antes [En este escenario, captive\_portal]
- Tipo: HTTP Basic (en este escenario de ejemplo)

Order Title 1 v ad_captive	AD Identity Source Active_Directory ~	Action	ACTIVE AUTHENTICATION For HTTP connections only, prompt for authenticate against the specified iden	r username and password and tity source to obtain the user
Source / Destination Active authentication		PASSIVE AUTH     Identity Sources are needed	d h Server Certificate	_portal:885
SOURCE		ACTIVE AUTH Captive Portal is needed		
Zones + Networks	+ Ports	NO AUTH	Networks +	Ports/Protocols +
ANY ANY	ANY	ANY	ANY	ANY

Una vez que se crea la política de identidad como autenticación activa, se crea automáticamente una regla SSL, de forma predeterminada esta regla se configura como cualquiera con **Decrypt-Resign**, lo que significa que no hay modificaciones SSL en esta regla.

$\Box \rightarrow \bigcirc \text{SSL Decryption} \rightarrow \bigodot \text{Identity} \rightarrow \bigcirc \text{Security Intelligence} \rightarrow \bigcirc \text{NAT} \rightarrow \bigodot \text{Access Control} \rightarrow \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $											
SSL Decryption 1 rule Q Search							¢ +				
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
🕘 🔝 Identity Policy	Active Authentica	tion Rules 🧃									
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	۵.
SSL Native Rules	0										
SSL Native Rules  SSL Native Rules  There are no SSL Rules yet. Start by creating the first SSL rule. CREATE SSL RULE O ADD PRE-DEFINED RULES											

$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \bigcirc$ NAT $\rightarrow \oslash$ Access Control $\rightarrow$ $\circledast$ Intrusion											
SSL Decryption	The rules in generated f	n this section are au from rules in the ide	tomatically entity policy				Q Search				¢ +
	SSL decryp rules are al	nent active authenti otion rules are read- lways evaluated befo	cation. These only. These ore the SSL	DESTINATION							
# NAME	native rules	s. ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
a Identity Policy Act	ive Authenticat	tion Rules 🧻									
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	e.
SSL Native Rules ()											
				Th	ere are no SSL Ru	les yet.					
				Start	by creating the firs	t SSL rule.					
	Start by creating the first SSL rule. CREATE SSL RULE or ADD PRE-DEFINED RULES										

Paso 4. Crear regla de acceso en la política de control de acceso

Debe permitir el **puerto 885/tcp** que redirige el tráfico a la autenticación del portal cautivo. Navegue hasta **Políticas > Control de acceso** y agregue la regla de acceso.

+
—

Si necesita verificar si los usuarios se descargaron de AD, puede editar la regla de acceso y navegar a la sección **Usuarios**, luego en **USUARIOS DISPONIBLES**, puede verificar cuántos usuarios tiene el FDM.

Order Title				Action	
1 ∨ ad_capti	ive			Allow	×
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS				6	CONTRO
▼ Filter					lf you config address, yo membershig
Identity Sources	Groups Users	-	-		appropriate different ad
Active_Directory \	luis		•		network acc from one gr
Active_Directory \	ngfwtac				Ű
Special-Identities	-Realm \ No Authe	entica			
Active_Directory \	ren				
Active_Directory \	sfua				
Active_Directory \	testuser		•		
Create new Identity Realm	CANCEL	ОК			

Recuerde implementar los cambios de configuración.

### Verificación

Verifique que el dispositivo del usuario recibe la casilla de verificación cuando se desplaza a un sitio HTTPS.

S https://10.115.117.43:885/xauthi × +								
← → C () 10.115.117.43:885/x.auth?s=dOF7LRChg4FKX2BCiK46wfdQKDJMAXeaLGcyYeiycuc%3D&u=http%3A%2F%2Fwww.cisco.com%2F								
	Sign in https://10.115.117.43:885 Username   Password Sign in Cancel							

Introduzca las credenciales de AD del usuario.

https://10.115.117.43:885/x.auth? ×	+					
← → C (1) 10.115.117.43:88	5/x.auth?s=dOF7LRCh	ng4FKX2BCiK46wfd	QKDJMAXeaLGcyYeiycu	%3D&u=http%3A%2F%2F	www.cisco.com%2F	
				Sign in https://10.1 Username Password	15.117.43:885	Sign in Cancel
: Cisco - Networking, Cloud, and ⊂ x + → C	ucts Support & Learn	Partners Events & Vid	deos			Q L +
Kiva and Cis retai	sco: Creating include	Active exp	Noti of Kaseya VSA in supply-of See the action	hain attack. Read the Tatos bi	og næ	time to take the lead
	E Design Guides	A+ Find Training	දියි Learning & Certifications	() Software Downloads	දිරියි Cisco Community	Activate Windows Tech Support Cases

## Troubleshoot

Puede utilizar la secuencia de comandos **user\_map\_query.pl** para validar FDM tiene la asignación ip de usuario

user\_map\_query.pl -i x.x.x.x ---> for ip addresses root@firepower:~# user\_map\_query.pl -u ngfwtac WARNING: This script was not tested on this major version (6.6.0)! The results may be unexpected. Current Time: 06/24/2021 20:45:54 UTC Getting information on username(s)... \_ \_ \_ User #1: ngfwtac \_ \_ \_ TD: 8 Last Seen: 06/24/2021 20:44:03 UTC for\_policy: 1 Realm ID: 4 ------Database \_\_\_\_\_ ##) IP Address [Realm ID] 1) ::ffff:10.115.117.46 [4] ##) Group Name (ID) [realm: Realm Name (ID)] 1) Domain Users (12) [realm: Active\_Directory (4)] En el modo clish puede configurar:

system support identity-debug para verificar si la redirección es exitosa.

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 10.115.117.46
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 2
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Logging EOF for event from hardware with
rule id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 : Received EOF, deleting the snort
session.
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 deleting firewall session flags = 0x10003,
fwFlags = 0x114
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
```

```
params) with zones 2 -> 3, port 63784 -> 53, geo 16671760 -> 16671778
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 looked for user_id with realm_id 4 auth_type
2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 found active binding for user_id 8 in realm
4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 2023803385 user_id =
8 \text{ realm_id} = 4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 1,
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 50619 -> 443, geo 16671760 -> 16671778
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 looked for user_id with realm_id 4
auth_type 2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 found active binding for user_id 8 in
realm 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 matched auth rule id = 2023803385 user_id
= 8 \text{ realm_id} = 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 new firewall session
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 HitCount data sent for rule id: 1,
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 allow action
Referencia:
```

```
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity.html#id_71535
```

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptdfdm-identity-sources.html#task\_83008ECD0DBF4E388B28B6247CB2E64B