# Configuración de la autenticación de AD para clientes AnyConnect

### Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Diagrama y escenario de la red
Determinar DN Base I DAP v DN de Grupo
Crear grupos de AD y agregar usuarios a grupos de AD (opcional)
Copiar la raíz del certificado SSL I DAPS (solo se requiere para I DAPS o STARTTI S)
Rango de coninguración
Habilitar la política de identidad y configurar las políticas de seguridad para la identidad del
usuario
Configurar exención de NAT
Implementación
Verificación
Configuración final
Configuración AAA
Configuración de AnyConnect
Conexión con AnyConnect y verificación de las reglas de la política de control de acceso
Verificar con eventos de conexión FMC
Troubleshoot
Depuraciones
Depuraciones de LDAP en funcionamiento
No se puede establecer una conexión con el servidor LDAP
Enlace DN de inicio de sesión o contraseña incorrecta
El servidor LDAP no puede encontrar el nombre de usuario
Contraseña incorrecta para el nombre de usuario
Prueba AAA
Capturas de paquetes
Registros del Visor de sucesos de Windows Server

## Introducción

Este documento describe cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a Firepower Threat Defence (FTD).

### Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de red privada virtual (VPN) de RA en Firepower Manage Center (FMC)
- Configuración del servidor de protocolo ligero de acceso a directorios (LDAP) en FMC
- Active Directory (AD)
- Nombre de dominio completo (FQDN)
- Intersight Infrastructure Services (IIS)
- Protocolo de escritorio remoto (RDP)

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft 2016 Server
- FMCv con 6.5.0
- FTDv con 6.5.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

Este documento describe cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a Firepower Threat Defense (FTD), administrado por Firepower Management Center (FMC).

La identidad del usuario se utiliza en las políticas de acceso para restringir a los usuarios de AnyConnect a direcciones IP y puertos específicos.

### Configurar

Diagrama y escenario de la red



Windows Server está preconfigurado con IIS y RDP para probar la identidad del usuario. En esta guía de configuración, se crean tres cuentas de usuario y dos grupos.

Cuentas de usuario:

- Administrador de FTD: se utiliza como cuenta de directorio para permitir que el FTD se enlace al servidor de Active Directory.
- Administrador de TI: cuenta de administrador de prueba utilizada para demostrar la identidad del usuario.
- Usuario de prueba: cuenta de usuario de prueba utilizada para demostrar la identidad del usuario.

Grupos:

- Administradores de AnyConnect: grupo de prueba que se agrega al administrador de TI para demostrar la identidad del usuario. Este grupo solo tiene acceso RDP al servidor Windows Server.
- Usuarios de AnyConnect: grupo de prueba que se agrega para demostrar la identidad del usuario. Este grupo sólo tiene acceso HTTP al servidor Windows Server.

#### Configuraciones de Active Directory

Para configurar correctamente la autenticación de AD y la identidad del usuario en FTD, se requieren algunos valores.

Todos estos detalles deben crearse o recopilarse en el servidor de Microsoft para poder realizar la configuración en FMC. Los valores principales son:

• Nombre de dominio:

Este es el nombre de dominio del servidor. En esta guía de configuración, example.com es el nombre de dominio.

• Dirección IP/FQDN del servidor:

La dirección IP o FQDN utilizado para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS en FMC y FTD para resolver el FQDN.

En esta guía de configuración, este valor es win2016.example.com (que resuelve 192.168.1.1).

• Puerto del servidor:

El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizan el puerto TCP 389 para LDAP, y LDAP sobre SSL (LDAP) utiliza el puerto TCP 636.

CA raíz:

Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.

• Nombre de usuario y contraseña del directorio:

Se trata de la cuenta que utilizan FMC y FTD para enlazar con el servidor LDAP y autenticar usuarios y buscar usuarios y grupos.

Para ello se crea una cuenta denominada FTD Admin.

• Nombre distinguido (DN) de base y grupo:

El DN base es el FMC de punto de partida y el FTD indica a Active Directory que inicie la búsqueda y autenticación de usuarios.

Del mismo modo, el DN de grupo es el punto de partida. FMC indica a Active Directory dónde debe comenzar la búsqueda de grupos para la identidad del usuario.

En esta guía de configuración, el dominio raíz example.com se utiliza como DN base y DN de grupo.

Sin embargo, para un entorno de producción, utilizar un DN base y un DN de grupo dentro de la jerarquía LDAP es mejor.

Por ejemplo, esta jerarquía LDAP:



Si un administrador desea que los usuarios de la unidad organizativa Marketing puedan autenticar el DN base, se puede establecer en la raíz (example.com).

Sin embargo, esto también permite que el usuario 1 de la unidad organizativa Finance inicie sesión, ya que la búsqueda de usuarios comienza en la raíz y desciende hasta Finance, Marketing e Research.

DN base establecido en example.com



Para restringir el inicio de sesión al único usuario de la unidad organizativa Marketing y a continuación, el administrador puede establecer el DN base en Marketing.

Ahora solo el Usuario 2 y el Usuario 3 pueden autenticarse porque la búsqueda comienza en Marketing.

DN base establecido en Marketing



Tenga en cuenta que para un control más granular dentro del FTD para el que los usuarios pueden conectarse o asignar a los usuarios una autorización diferente en función de sus atributos AD, se debe configurar un mapa de autorización LDAP.

Puede encontrar más información al respecto aquí: <u>Configuración de la asignación LDAP de</u> <u>AnyConnect en Firepower Threat Defence (FTD)</u>.

Esta jerarquía LDAP simplificada se utiliza en esta guía de configuración y el DN para la raíz example.com se utiliza tanto para el DN base como para el DN de grupo.



Determinar DN Base LDAP y DN de Grupo

1. Abra Usuarios y equipos de Active Directory.



, haga clic con el botón secundario en el contenedor o unidad organizativa al que se agrega el nuevo grupo.

En este ejemplo, el grupo AnyConnect Admins se agrega bajo el contenedor Users. Haga clic con el botón derecho en Users y navegue hasta New > Group.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 🚾 🔏 🖬 🗶	3 🙆 📑 🖬 🖬	e 🗏 🐮 🛯	r 🧕 🕱		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers Signature Accourt Managed Service Accourt Users Delegate Con Find New All Tasks View	Name DefaultAcco DefaultAcco DonsUpdateRoll DonsUpdateP Domain Ad Domain Co ntrol e ers	Type Descrip User A user Security Group Memb Security Group DNS A Security Group DNS cl Security Group Design Security Group All wor Security Group All dor Security Group All dor	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		^
Refresh Export List		InetOrgPerson msDS-KeyCreder msDS-ResourceP	ntial PropertyList		
Properties		msDS-ShadowPr	incipalContainer		
K State Stat	Read-only Schema A	msImaging-PSPs MSMQ Queue Al Printer User Shared Folder	ias .		~
Creates a new item in this container.		strated rotati			

2. Vaya al asistente Nuevo objeto - Grupo.

New Object - Group		×
Create in: example.com,	Users	
Group name:		
AnyConnect Admins		
Group name (pre-Windows 2000):		
AnyConnect Admins		
Group scope	Group type	
O Domain local	Security	
Global	Olistribution	
OUniversal		
	OK Cancel	

3. Compruebe que se ha creado el grupo. También se crea el grupo Usuarios de AnyConnect.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🖄 📰 🕹 🔛 🗉	è   🛛 🖬   🐍 🗽 🛍 '	7 🧕 🗽			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Sign Domain Controllers Sign ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount DefaultAccount DonsIpdateProxy DonsUpdateProxy DonsUpdateProxy Domain Computers Domain Computers Domain Controllers Domain Controllers Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User User User	Description Built-in account for ad Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		
	(Ba.s				

4. Haga clic con el botón derecho del ratón en el grupo de los usuarios y, a continuación, seleccione Propiedades. En esta configuración, el usuario IT Admin se agrega al grupo AnyConnect Admins y el usuario Test User se agrega al grupo AnyConnect Users.

File Action View Help	
수 수 🖄 📅 🔏 🗈 🗙 🗑 🕢 💀 📓 📅 🕱 🔌 🗑 🝸 🗕 🔌	
Active Directory Users and Com     Name     Type     Description	^
✓ initial example.com       AnyConnect Users       Security Group       Add to a group         > initial builtin       Computers       Security Group       Built         > initial computers       Computers       Security Group       Move         > initial computers       Cert Publishers       Security Group       Mer         > initial computers       Security Principal:       Add to a group         > initial computers       Security Group       Mer         > initial complexently Principal:       Conceable Domain C       Security Group       Mer	
Managed Service Accourt     DefaultAccount     User     Au     DefaultAccount     DefaultAccountAcount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccountAcount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccount     DefaultAccountAcount     DefaultAccountAcount     DefaultAccount     DefaultAccountAcount     DefaultAccountAcount     DefaultAccountAcount     DefaultAccountAcount     DefaultAccountAcount	
Image: Domain Guests       Security Group       All domain users         Image: Domain Users       Security Group       All domain users         Image: Domain Users       Security Group       All domain users         Image: Domain Users       Security Group       Designated administrato         Image: Domain Users       Security Group       Members of this group         Image: Domain User       Security Group       Members of this group         Image: Domain User       Security Group       Members in this group c         Image: Domain User       Security Group       Members in this group c         Image: Domain Designated administrato       Security Group       Members of this group c         Image: Domain Designated administrato       Security Group       Members of this group c         Image: Domain Designated administrato       Security Group       Members of this group c         Image: Domain Designated administrato       Security Group       Members of this group c         Image: Domain Designated administrato       Security Group       Members of this group c         Image: Domain Designated administrato       Security Group       Members of this group	
	~

5. En la pestaña Miembros, haga clic en Agregar.

AnyConnect Admins	Properties			?	×
General Members	Member Of	Managed By			
Members:					
Name	Active Dir	ectory Domain	Services Folder		
Add	Remove				
		ОК	Cancel	A	ply

Introduzca el usuario en el campo y haga clic en Comprobar nombres para comprobar que se ha encontrado el usuario. Una vez verificado, haga clic en Aceptar.

Select Users, Contacts, Computers, Service Accounts, or Gro	oups X
Select this object type: Users, Service Accounts, Groups, or Other objects	Qbject Types
From this location: example.com	Locations
Enter the object names to select ( <u>examples</u> ): IT Admin (it admin@example.com)	Qheck Names
Advanced	OK Cancel

Compruebe que se ha agregado el usuario correcto y haga clic en Aceptar. El usuario Test User también se agrega al grupo AnyConnect Users siguiendo los mismos pasos.

AnyConnect Admin	s Properties			?	×
General Members	Member Of	Managed B	У		
Members:					
Name LT Admin	Active Dir example o	ectory Domai com/Users	n Services Folde	r	
Add	Remove				
		OK	Cancel	Aç	<b>ply</b>

Copiar la raíz del certificado SSL LDAPS (solo se requiere para LDAPS o STARTTLS)

1. Presione Win+R e ingrese mmc.exe. Luego haga clic en OK (Aceptar).



2. Vaya a Archivo > Agregar o quitar complemento.

🔚 Cor	nsole1 - [Console Root]			-		×
File File	Action View Favorites	Window	Help		-	8 ×
\$	New	Ctrl+N				
	Open	Ctrl+O	Actions			
	Save Save	Ctrl+S	There are no items to show in this view, Console Root			-
	Save AS		More Actions			٠
	Add/Remove Snap-in	Ctrl+M				
	Options					
	1 dnsmgmt					
	2 059					
	Dot					
Enables	you to add snap-ins to or remo	ove them fro	m the snap-in console.			

3. En Complementos disponibles, seleccione Certificados y haga clic en Agregar.

iap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Demous
Active Directory Site	Microsoft Cor			Remove
Active Directory Use	Microsoft Cor			
ActiveX Control	Microsoft Cor			Move <u>U</u> p
ADSI Edit	Microsoft Cor			Moura Destra
Authorization Manager	Microsoft Cor		Add >	Hove Fown
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and	¥		Advanced

4. Seleccione Cuenta de computadora y haga clic en Siguiente.

Certificates snap-in	×
This snap-in will always manage certificates for: <u>Service account</u> <u>Computer account</u>	
< <u>B</u> ack <u>N</u> ext >	Cancel

Haga clic en Finish (Finalizar).

Select Computer	$\times$
Select the computer you want this snap in to manage.         This snap in will always manage: <ul> <li>Local computer: (the computer this console is running on)</li> <li>Another computer:</li> <li>Another computer:</li> <li>Browse</li> </ul> Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5. Haga clic en Aceptar.

Cor Cor Cor			uge Certificates (Local Computer)	<u>R</u> emove
Cor Cor				
Cor				
Cor				Marca 11
				Move Up
.or				Move Down
.or		<u>A</u> dd >		
Cor				
and	~			Advanced
	tor tor tor tor tor tor tor	tor tor tor tor tor tor tor	Cor Cor.	tor Add > Add > Cor Add

6. Expanda la carpeta Personal y, a continuación, haga clic en Certificados. El certificado utilizado por LDAPS se emite para el nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay 3 certificados listados.

- Un certificado de CA emitido a y por ejemplo-WIN2016-CA.
- Certificado de identidad emitido para WIN2016 por example-WIN2016-CA.
- Certificado de identidad emitido para win2016.example.com por example-WIN2016-CA.

En esta guía de configuración, el FQDN es win2016.example.com y, por lo tanto, los 2 primeros certificados no son válidos para su uso como certificado SSL LDAP. El certificado de identidad emitido para win2016.example.com es un certificado emitido automáticamente por el servicio de CA de Windows Server. Haga doble clic en el certificado para comprobar los detalles.



7. Para ser utilizado como certificado SSL LDAPS, el certificado debe cumplir estos requisitos:

- El nombre común o el nombre alternativo de sujeto DNS coincide con el FQDN del servidor de Windows.
- El certificado tiene Autenticación del servidor en el campo Uso mejorado de clave.

En la pestaña Detalles del certificado, seleccione Asunto y Nombre alternativo del sujeto, el FQDN win2016.example.com está presente.

🙀 Certificate	×
General Details Certification Path	
Show: <all></all>	$\sim$
Field	Value ^
Subject	win2016.example.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Name	DomainController
Enhanced Key Usage	Client Authentication (1.3.6.1
SMIME Capabilities	[1]SMIME Capability: Object I
Subject Key Identifier	30 b7 2b 4e 48 0f 2f 17 17 e6
2001 Authority Key Identifier	KevID=3d 9f 26 37 th 11 1f 4
CN = win2016.example.com	
Ec	It Properties Copy to File
	01
	UK

En Enhanced Key Usage, Server Authentication está presente.

Certificate	×
General Details Certification Pat	th
Show: <ai></ai>	$\sim$
Field	Value ^
Subject	win2016.example.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Name	DomainController
Enhanced Key Usage	Client Authentication (1.3.6.1
SMIME Capabilities	[1]SMIME Capability: Object I
Subject Key Identifier	30 b7 2b 4e 48 0f 2f 17 17 e6
Authority Key Identifier	KeyID = 34 9f 26 37 fb 11 1f 4
Client Authentication (1.3.6.1.5. Server Authentication (1.3.6.1.5.	5.7.3.2) .5.7.3.1)
	Edit Properties Copy to File
	OK

8. Una vez confirmado, en la pestaña Ruta de certificación, seleccione el certificado superior que es el certificado de CA raíz y, a continuación, haga clic en Ver certificado.

💼 Certificate	×
General Details Certification Path	
Certification path	
win2016.example.com	
	View Certificate
Certificate status:	
This certificate is OK.	
	ОК

9. Se abrirán los detalles de Certificados para el certificado de CA raíz.

Certificate	×
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s): Al issuance policies Al application policies	
Issued to: example-WIN2016-CA	
Issued by: example-W/IN2016-CA	
Valid from 4/27/2020 to 4/19/2060	
Issuer Statement	1
OK	

En la pestaña Details, haga clic en Copy to File.

💼 Certificate		×
General Details Certification Path	1	
Show: <al></al>	$\sim$	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Subject	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA sha256 example-WIN2016-CA Monday, April 27, 2020 10:50: Monday, April 19, 2060 10:50: example-WIN2016-CA	¥
E	dit Properties	
	OF	¢

10. Vaya al Asistente para exportación de certificados. El asistente exporta la CA raíz en formato PEM.

🔶 😺 Certificate Export Wizard	×
Welcome to the Certificate Export Wizard	
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
To continue, click Next.	
Next Cancel	

Seleccione Base-64 codificado X.509.

← 4	🚰 Certificate Export Wizard	×
_	Export File Format Certificates can be exported in a variety of file formats.	
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	Include all certificates in the certification path if possible	
	Personal Information Exchange - PKCS #12 (.PFX)	
	Include all certificates in the certification path if possible	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	Microsoft Serialized Certificate Store (.SST)	
	Next Cancel	

Seleccione el nombre del archivo y a dónde se exporta.

		$\times$
÷	F Certificate Export Wizard	
	File to Export	
	specify the name of the ne you want to export	
		_
	File name:	
	Browse	
	Next Cancel	

🚟 Save As					×
← → ~ ↑ 💻	> This PC > Desktop		✓ Ö Search Des	ktop	<i>م</i>
Organize 🔻 Nev	v folder			()EE	• 🕐
🔹 Quick access	Name	Date modified	Туре	Size	
Desktop	A	No items match your sea	rch.		
🕹 Downloads	A				
🗄 Documents	*				
Pictures	*				
System32					
💻 This PC					
💣 Network					
File name:	root				~
Save as type:	Base64 Encoded X.509 (*.cer)				~
∧ Hide Folders			Save	. C	ancel

		Х
←	🚱 Certificate Export Wizard	
	Specify the name of the file you want to export	
	Fie came:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cance	d

Ahora haga clic en Finish.



11. Desplácese hasta la ubicación y abra el certificado con un bloc de notas u otro editor de texto. Muestra el certificado de formato PEM. Guarde esto para más tarde.

#### ----BEGIN CERTIFICATE----

MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJ1eGFtcGx1LVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDAOMTkxNDUwNT1aMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV 00+k6dVVY/E5qVkEKSGoY+v940S23161zdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3C0+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM aob4XE/0zxYQpPa18djsNnskfcFqD/HOTFQN4+Sr0hHW1RnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKq0L7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00 BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xp11IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DgZg+R96 9WLCR30big6xyo9Zu+1ixcWpdrbAD06zMhbEYEhkh00jBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33Pp1W6E -----END CERTIFICATE-----

12. (Opcional) En el caso de que haya múltiples certificados de identidad que puedan ser utilizados por LDAPS y haya incertidumbre sobre cuál se utiliza, o no haya acceso al servidor LDAPS, es posible extraer la ca raíz de una captura de paquetes realizada en el servidor Windows o FTD después.

Configuraciones de FMC

Verificar licencia

Para implementar la configuración de AnyConnect, el FTD debe estar registrado con el servidor de licencias inteligentes, y se debe aplicar al dispositivo una licencia válida Plus, Apex o VPN Only.

1. Vaya a System > Licenses > Smart Licensing.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deplo	y 🔒 🛛	System	Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Mon	itoring 🔻	Tools •
										Sm	art Licenses ssic Licenses				

2. Compruebe que los dispositivos cumplen los requisitos y que se han registrado correctamente. Asegúrese de que el dispositivo esté registrado con una licencia AnyConnect Apex, Plus o VPN Only License.

(	Overview	Analysis	Policies	Devic	es Objects	AMP	Intelligence				Deploy	• •	System Help 🔻	admin 🔻
					0	onfiguratio	n Users	Domains	Integration	Updates	Licenses + Smart Licenses	Health	<ul> <li>Monitoring •</li> </ul>	Tools <b>*</b>
	Smart L	icense Sta	atus					Cisco Se	art Software Mana	un 🔴 🧶				
	Usage Aut	horization:		© ^	thorized (Last S)	mchronized (	On Nay 03 2020)							
	Product Re	gistration:		Ø R	gistered (Last Re	newed On M	lar 03 2020)							
	Assigned V	/irtual Accour	it:	2	C TAC									
	Export-Co	ntrolled Featu	anesi:	Er	bled									

Smart Licenses			Filter Devices		× Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group
Firepower Management Center Virtual (2)	0				
) 💭 Base (2)	0				
<sup>b</sup> G Mahware (1)	٥				
<sup>b</sup> <sup>[2]</sup> Threat (2)	0				
<sup>b</sup> <sup>2</sup> URL Filtering (2)	٢				
≠ G AnyConnect Apex (1)	0				
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	0	Cisco Firepower Threat Defen	se for VMWare	Global	N/A
AnyConnect Plus (0)					
AnyConnect VPN Only (0)					

#### Rango de configuración

Cisco Success Network:

Cisco Support Diagnostics:

Disabled 🕕

Disabled 🕕

1. Vaya a Sistema > Integración.

Overview A	Analysis	Policies	Devices	Objects	АМР	Intelligence					Deploy	/ 🔍 🔊	ystem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health *	Monitoring •	Tools *

2. En Rangos, haga clic en Nuevo rango.

Overview Analysis Policie	s Devices Objects	AMP Intelligenc	e				Deploy	0 Sys	tem Help +	admin 🔻
		Config	uration Users	Domains	Integration	Updates	Licenses 🔻	Health <b>v</b>	Monitoring	<ul> <li>Tools *</li> </ul>
Cloud Services Realms	Identity Sources e	Streamer Host Ing	out Client Sm	art Software S	atellite					
🖌 Compare realms 🕓 New real										
Name	Description	Domain	Туре	Base DN	Group	DN	Group Attri	ibute	State	

3. Rellene los campos correspondientes según la información recopilada del servidor de Microsoft. Luego haga clic en OK (Aceptar).

#### Add New Realm

Name *	LAB-AD	
Description		
Type *	AD	v
AD Primary Domain *	example.com	ex: domain.com
AD Join Username		ex: user@domain
AD Join Password		Test AD Join
Directory Username *	ftd.admin@example.com	ex: user@domain
Directory Password *	•••••	
Base DN *	DC-example,DC-com	ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	Y
* Dequired Field		
· Keyuneu riela		
		OK Cancel

4. En la nueva ventana, seleccione Directorio si aún no está seleccionado, pulse Añadir directorio.

Overview	Analysis	Policies	Devices	Objects AM	P Intellig	ntelligence Deploy 🤤 System						admin <del>v</del>
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health <b>v</b>	Monitoring •	Tools •
LAB-AD	ion										Save	Cancel
Directory	Realm Con	figuration	User Down	nload								
											04	dd directory

Rellene los detalles del servidor de AD. Tenga en cuenta que si se utiliza el FQDN, FMC y FTD no se podrán enlazar correctamente a menos que DNS esté configurado para resolver el FQDN.

Para configurar DNS para FMC, navegue hasta System > Configuration y seleccione Management Interfaces.

Para configurar DNS para el FTD, navegue hasta Devices > Platform Settings, cree una nueva política o edite una actual y luego vaya a DNS.

Add directory	?	×
Hostname / IP Address	win2016.example.com	
Port	389	
Encryption	○ STARTTLS ○ LDAPS ④ None	
SSL Certificate	<ul> <li>✓ ②</li> </ul>	
	OK Test Cancel	

Si se utiliza LDAPS o STARTTLS, haga clic en el símbolo verde + (más), asigne un nombre al certificado y copie el certificado de CA raíz con formato PEM. A continuación, haga clic en Guardar.

Import <sup>·</sup>	Trusted Certificate Authority	? ×
Name:	LDAPS_ROOT	
Certificat	ate Data or, choose a file: Browse	
BEGI MIIDCDC MRswGQ MjA2MD/ ASIwDQV Ya+Pngs OO+k6dV Cjyeub3C aob4XE/0 sVs5PneV AwEAAaN BBYEFD2 vzwVD3C phFIHZo0 6tALTt3A dLEFKQq 9WLCR30 KgwBJXE END	SIN CERTIFICATE CCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd QYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP A0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC PYJKoZIhvcNAQEBBQADgEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b sxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV VVY/E5qVkEKSG0Y+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM /OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/ PYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C NCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O 2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r bCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D qmMeYvkVf+a7a64mqPZsG3Ux00rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 8Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk Eu33PplW6E 0 CERTIFICATE	
	Save	Cancel
		Janoa

Seleccione la CA raíz recién agregada en el menú desplegable junto a Certificado SSL y haga clic en STARTTLS o LDAPS.

Edit directory	?	×
Hostname / IP Address	win2016.example.com	
Port	636	
Encryption	○ STARTTLS	
SSL Certificate	LDAPS_ROOT 💙 📀	
	OK Test Cancel	

Haga clic en Test (Probar) para asegurarse de que FMC se puede enlazar correctamente con el nombre de usuario y la contraseña del directorio proporcionados en el paso anterior.

Dado que estas pruebas se inician desde el FMC y no a través de una de las interfaces enrutables configuradas en el FTD (como interna, externa o dmz), una conexión correcta (o fallida) no garantiza el mismo resultado para la autenticación de AnyConnect porque las solicitudes de autenticación LDAP de AnyConnect se inician desde una de las interfaces enrutables del FTD.

Para obtener más información sobre la prueba de conexiones LDAP del FTD, revise las secciones Prueba de AAA y Captura de paquetes en el área de resolución de problemas.



5. En User Download, descargue los grupos que se utilizan para la identidad del usuario en pasos posteriores.

Marque la casilla Descargar usuarios y grupos y la columna de Grupos disponibles se rellena con los grupos configurados en Active Directory.

Los grupos pueden ser Incluidos o Excluidos; sin embargo, de forma predeterminada, se incluyen todos los grupos que se encuentran en el DN de grupo.
También se pueden incluir o excluir usuarios específicos. Los grupos y usuarios incluidos estarán disponibles para seleccionarlos posteriormente para la identidad del usuario.

Cuando haya terminado, haga clic en Guardar.

Overview Analysis Policies Devices Objects A	AMP Intellige	nce						Deploy	0 Sys	tem Help 🔻	admin <del>v</del>
	Conf	figuration	Users	Domains	Integration	Upd	lates	Licenses 🔻	Health <b>*</b>	Monitoring •	Tools <b>*</b>
LAB-AD Enter Description								You have un	saved changes	E Save	2 Cancel
Directory Realm Configuration User Download											
Download users and groups											
Begin automatic download at 8 V PM V America/New York	Repeat Every 24	✓ Hours									
Download Now											
Available Groups 🖒	G	iroups to Ind	lude (2)				Group	s to Exclude (	0)		
a Search by name	4	🛃 AnyConnec	t Admina			- 6	None				
AnyConnect Admins	4	🔗 AnyConnec	t Users			8					
A DrisUpdateProxy											
A WseRemoteAccessUsers											
A WseInvisibleToDashboard											
Allowed RODC Password Replication Group	Add to										
A Enterprise Key Admins	Indude										
🝰 Domain Admins	Add to										
A WseAlertAdministrators	Exclude										
🝰 Event Log Readers											
A Replicator											
🝰 Domain Guests											
A Windows Authorization Access Group											
Account Operators											
🛃 Hyper-V Administrators 🗸 🗸 🗸											-
👶 System Managed Accounts Group		Enter User Ind	fusion			Add	Enter	User Exclusion			Add

#### 6. Active el nuevo rango.

Overview Analysis Policie	es Devices Objec	ts AMP I	ntelligence						Deploy	0, Sy	stem Hel	p <del>▼</del> admin <del>▼</del>
			Configurat	ion Us	ers Domai	is Integr	ation	Updates	Licenses <b>*</b>	Health <b>*</b>	Monitoria	ng 🔻 🛛 Tools 🔻
Cloud Services Realms	Identity Sources	eStreamer	Host Input	Client	Smart Softw	are Satellite						
										Comp	are realms	New realm
Name	Description	Domain	т	ype	Base DN		Group D	N	Group Attr	ibute	State	
LAB-AD		Global	A	D	DC=examp	le,DC=com	DC=exan	ple,DC=com	member			ተ 🖉 🗗 🖯

7. Si se utiliza LDAPS o STARTTLS, el FTD también debe confiar en la CA raíz. Para hacer esto, primero navegue hasta Dispositivos > Certificados.

Overview Analysi	s Policie	es Dev	ices	Objects	AMP J	Intelligence		Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V	Q0S	Platform	n Settings	FlexConfig	Certificates					

Haga clic en Agregar en la esquina superior derecha.

Overview Analysis	Policie	es Dev	ices	Objects	АМР	Intelligence		Deploy	0,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN +	QoS	Platform	Setting	s FlexConfig	Certificates					
											0	A44

Seleccione el FTD, se añade la configuración LDAP a y, a continuación, haga clic en el símbolo + (más).

Add New Certificate		? ×
Add a new certificate to the identify certificate.	e device using cert enrollment object whi	ch is used to generate CA and
Device":	FTD-2	×
Cert Enrollment*:	Select a certificate entrollment object	× 🖸
		Add Cancel

Dé un Nombre al punto de confianza y, a continuación, seleccione Inscripción manual en el menú desplegable Tipo de inscripción. Pegue aquí el certificado de CA raíz PEM y haga clic en Guardar.

Add Cert Enrollmer	nt	? ×
Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual 🗸	^
CA Certificate:*	<ul> <li>BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki</li> <li>G9w0BAQsFADAd</li> <li>MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI</li> <li>MMTQ1MDU5WhgP</li> <li>MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU</li> <li>tv0lOMjAxNi1DQTCC</li> <li>ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N</li> <li>zSQpoQPh0YT67b</li> <li>Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf</li> <li>d++M+bLn3AiZnHV</li> <li>OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo</li> <li>ficrRhihonuU</li> <li>Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN</li> <li>O7KEMkfA1LPuM</li> <li>aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU</li> <li>aLdQaabhipD/</li> <li>sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKgOL7N86</li> </ul>	~
Allow Overrides		
	Save	Cancel

Compruebe que el punto de confianza creado está seleccionado y haga clic en Agregar.

Add New Certificate		? ×
Add a new certificate to th identify certificate.	e device using cert enrollment object whic	ch is used to generate CA and
Device*:	FTD-2	<b>~</b>
Cert Enrollment*:	LDAPS_ROOT	<b>~</b> ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

El nuevo punto de confianza aparece bajo el FTD. Aunque menciona que se requiere la importación del certificado de identidad, no es necesario que el FTD autentique el certificado SSL enviado por el servidor LDAPS. Por lo tanto, este mensaje puede ser ignorado.

Overview Analysis	Policies Devices	Objects AMP Int	telligence	Deploy 🔒	System Help 🔻 admin 🔻
Device Management	NAT VPN • Qos	5 Platform Settings	FlexConfig Certificates		
					Add 🔘
Name	Domain	Enrollment Typ	oe Status		
4 🗐 FTD-1					
FTD-1-PKCS12	Global	PKCS12 file	CA 🔍 ID		P 🗘 🖥
4 🗐 FTD-2					
FTD-2-PKCS12	Global	PKCS12 file	CA 🔍 ID		P ¢ 🖩
FTD-2-Selfsigned	Global	Self-Signed	S CA LD		12 ¢ 🗎
LDAPS_ROOT	Global	Manual	🔍 CA 🛛 🔺 Ide	ntity certificate import require	sd ₽¢ 🖩

Configuración de AnyConnect para la autenticación de AD

 En estos pasos se supone que no se ha creado ya ninguna directiva VPN de acceso remoto. Si se ha creado una, haga clic en el botón edit (editar) de dicha directiva y vaya directamente al paso
 3.

Vaya a Devices > VPN > Remote Access.



Haga clic en Agregar para crear una nueva Política VPN de acceso remoto

Overview An	alysis Poli	des Devices	Objects	AMP	Intelligence				Deploy	e,	System	Help 🔻	admin <del>v</del>
Device Managem	nent NAT	VPN + Remo	te Access	Qo5	Platform Settings	FlexConfig	Certificates						
												0	Add
Name					Status		Las	t Modified					
				N	o configuration a	vailable Add	t a new conf	figuration					

2. Complete el Asistente para directivas VPN de acceso remoto. En Asignación de directiva, especifique un nombre para la directiva y los dispositivos a los que se aplica la directiva.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy	y 🔒 System Help 🕶 admin 🕶
Device Management NAT VPN • Remote Access QoS Platform Settings FlexConfig Certificates	
Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary	
Targeted Devices and Protocols	
This witard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.	
Before you start, ensure t configuration elements to b	the following e in place to
Name:* PTD-2-RA-Policy	Policy.
Description: Configure Bealm or BADIUS	Server Group
VPN Protocols: SSL I IPsee-IKEv2	
Targeted Devices: Available Devices Selected Devices Neke sure you have AnyCom	nect package
Search and	or you have s to download
FTD-1	
Device Interface Interfaces should be already	configured on
targeted <u>devices</u> so that they as a security zone or interf	/can be used ace group to
enable VPN access.	
Add	
	`
Back	Next Cancel

En Perfil de conexión, especifique el nombre de Perfil de conexión que también se utiliza como alias de grupo que los usuarios de AnyConnect ven cuando se conectan.

Especifique el rango creado previamente en Servidor de autenticación.

Especifique el método mediante el cual se asignan direcciones IP a los clientes de AnyConnect.

Especifique la directiva de grupo predeterminada que se utiliza para este perfil de conexión.

Overview Analysis Policies Devices Objects AMP	Intelligence		Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access QoS	Platform Settings FlexConfig	Certificates		
Remote Access VPN Policy Wizard				
Policy Assignment     O Connection Profile     3	AnyConnect 🔪 🕢 Access 8	Certificate S Summary		
Connection Profile:				^
Connection Profiles specify the tunne accomplished and how addresses are	group policies for a VPN connection. The assigned. They also include user attribut	se policies pertain to creating the tunnel itself, ho es, which are defined in group policies.	w AAA is	
Connection Profile Name:*	General	]		
	This name is configured as a connection all	as, it can be used to connect to the VPN gateway		
Authentication, Authorization & A Specify the method of authentication	ccounting (AAA): (AAA, certificates or both), and the AAA	servers that will be used for VPN connections.		
Authentication Nethod:	AAA Only 🛩			
Authentication Server:*	LAB-AD 👻	G+ (Realm or RADIUS)		
Authorization Server:	×	G (RADIUS)		
Accounting Server:	¥	(RADIUS)		
Client Address Assignment: Client IP address can be assigned fro assignment is tried in the order of AA	m AAA server, DHCP server and IP addres A server, DHCP server and IP address po	ss pools. When multiple options are selected, 1P a ol.	ddress	
Use AAA Server (RADUUS ) Use DHCP Servers Use IP Address Pools	inly) 🕕			
IPv4 Address Pools:	AnyConnect-Pool	1		
IPv6 Address Pools:		1		
Group Policy: A group policy is a collection of user- or create a Group Policy object.	oriented session attributes which are assi	gned to client when a VPN connection is establish	ed. Select	
Group Policy:*	DfitGrpPolicy	a		
	car way rong			¥
			Back Next	Cancel

En AnyConnect, cargue y especifique los paquetes de AnyConnect que se utilizan.

Overview Analysis Polici	ies	Devices Objects	AMP	Intelligence					Deploy	0 <sub>5</sub> System	Help 🔻	admin <del>v</del>
Device Management NAT	v	PN • Remote Access	QoS	Platform Settings	FlexConfig	Certific	ates					
Remote Access VPN P	Poli	cy Wizard										
1 Policy Assignment	2	) Connection Profile	3	AnyConnect (	Access &	Certifica	ite 📏 🕥 Sumn	hary				
	Any The initi	Connect Client Image VPN gateway can automatic ated. Minimize connection set	tup time b	load the latest AnyConr y choosing the appropria	ect package to ite OS for the se	the client of lected pack	levice when the VPN or age.	onnection is				^
	Dow	nload AnyConnect Client pac	kages fro	m Cisco Software Downlo	ad Center.		how De-order buttons	0				
	1	AnyConnect File Object	Name	AnyConnect Client	Package Name		Operating System	Ĭ				
	2	anyconnect-linux64-4.7.03	052-we	anyconnect-linux64-4	.7.03052-webde	ploy-k9	Linux	*				
	2	anyconnect-win-4.7.00136	i-webde	anyconnect-win-4.7.0	0136-webdeploy	-k9.pkg	Windows	*				~
									Back	- North		-
									Back	Next		incel

En Acceso y certificado, especifique la interfaz a la que acceden los usuarios de AnyConnect para AnyConnect.

Cree y/o especifique el certificado que utiliza el FTD durante el intercambio de señales SSL.

Asegúrese de que la casilla de verificación Omitir la política de control de acceso para el tráfico descifrado (sysopt permit-vpn) esté desactivada para que la identidad de usuario creada más adelante surta efecto para las conexiones RAVPN.



#### En Summary, revise la configuración y haga clic en Finish.



3. En la directiva VPN > Acceso remoto, haga clic en el icono Edit (lápiz) para obtener el perfil de conexión correspondiente.

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻
Device Management NAT VPN > Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Save
Connection Reality Access Teterforms Advanced		Policy Assignments (1)
Connection Profile Access Interfaces Advanced		
		G
Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	👔 DfkGrpPolicy 🥒 🗊
General	Authentication: LAB-AD (AD) Authorization: Identi Accounting: Identi	Pi OftGrpPolicy

Asegúrese de que el Servidor de autenticación esté configurado en el rango creado anteriormente.

En Advanced Settings, se puede marcar Enable Password Management para permitir que los usuarios cambien su contraseña cuando o antes de que caduque.

Sin embargo, esta configuración requiere que el rango utilice LDAPS. Si se ha realizado algún cambio, haga clic en Guardar.

Edit Connection Profile		? ×					
Connection Profile:* Genera Group Policy:* DfltGrp Edit Grou	General DfltGrpPolicy Edit Group Policy						
Client Address Assignment	AAA Aliases						
Authentication							
Authentication Method:	AAA Only						
Authentication Server:	LAB-AD (AD)						
Use secondary authentica Authorization Authorization Server:	tion          Image: Constraint of the second state of the secon						
Accounting							
Accounting Server:	▼						
Advanced Settings Strip Realm from usernam Strip Group from usernam Enable Password Manage Notify User 14 days Notify user on the day of	ne ment prior to password expiration						
	Save Cance						

Cuando haya terminado, haga clic en Guardar.

Overview Analysis	Polici	es Devices Objects	AMP	Intelligence			Deploy 🔍 System Help 🔻 admin 🔻
Device Management	NAT	VPN • Remote Access	QoS	Platform Settings	FlexConfig	Certificates	
FTD-2-RA-Pol	су						You have unsaved changes 📔 Save 🛛 🔞 Cancel

Habilitar la política de identidad y configurar las políticas de seguridad para la identidad del usuario

1. Vaya a Políticas > Control de acceso > Identidad.



Cree una nueva política de identidad.



Especifique un nombre para la nueva política de identidad.

New Identit	y policy ? ×
Name	FTD-2 Identity Policy
Description	
	Save Cancel

#### 2. Haga clic en Agregar regla.

Overvie	w Analysis Pol	icies Devices	s Objects	AMP Intellig			De	ploy 🔒 Syste	m Help <del>v</del>	admin 🔻		
Access	Control > Identity	Network Disc	overy Appli	cation Detectors	Correlation	Actions <b>*</b>						
FTD-2 Enter Desc	FTD-2 Identity Policy											
Rules	Active Authentication											
	Add Category O Add Rule Search Rules X											
# Name		Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Prote	col

3. Especifique un nombre para la nueva regla. Asegúrese de que esté habilitado y de que la acción esté configurada como Autenticación Pasiva.

Haga clic en la pestaña Rango y configuración y seleccione el rango creado anteriormente. Haga clic en Agregar cuando haya terminado.

Add Rule

Name	RAVPN			🖌 Enabled	Insert	into Category	~	Standard Rules	~
Action	Passive Authentica	ition	~	Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude	HTTP User-	Agents: None	
	Remote access VPN	sessions are a	ctively authentic	cated by VPN. Other sessions	s use the rule Action.				
Zone	s Networks	VLAN Tags	Ports					Realm &	Settings
Realm	•	LAB-AD (AD	2)						
	active authenticati	on if passive or	VPN identity ca	rooot he established	6°				
	e active authenticati	orr in passive or	very identity ca	ninot be established					
* Requ	uired Field								
								Add	Cancel

#### 4. Haga clic en Guardar.

0	verview Analysis Poli	icies Device	s Objects	AMP Intelli	gence				Dep	xloy 🧛 System	Help 🔻 adn	nin <del>v</del>
A	cess Control + Identity	Network Disc	overy Appl	cation Detectors	Correlation	Actions •						
F	FTD-2 Identity Policy You have unsaved changes Save Cancel											
Ru	Rules Active Authentication											
							Add Categor	y ( 🔾 Add Rule	Search Rules		×	
	Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Adr	ninistrator Rules											
Thi	s category is empty											
Sta	ndard Rules											
1	RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentication	none	/8
Roo	t Rules											
The	s category is empty											

Displaying 1 - 1 of 1 rules  $|\langle \langle Page | 1_{-} of 1 \rangle > |$ 

5. Acceda a Políticas > Control de Acceso > Control de Acceso.



6. Edite la política de control de acceso en la que se ha configurado el FTD.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	e, s	iystem	Help 🔻	admin <del>v</del>
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions <b>*</b>						
					Object Management Intro	usion Netwo	rk Analys	is Policy	DNS Im	port/Export
									O Nev	v Policy
Access Control Policy		Status			Last Modified					
Default-Policy		Targeting 1 de Up-to-date on	vices all targeted device	5	2020-05-04 09:15:56 Modified by "admin"				<b>G</b> B	28

7. Haga clic en el valor junto a Política de identidad.

Overview Analysis Policies	Devices Objects	AMP Intelligence			Deploy 🧕 System Help 🔻 admin 🔻
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions <b>*</b>	
Default-Policy Enter Description					Analyze Hit Counts 🔡 Save 🖸 Cancel
Prefilter Policy: Default Prefilter Policy		SSL	Policy: None		Identity Policy: None
					Te Inheritance Settings   📉 Policy Assignments (1)

Seleccione la política de identidad creada anteriormente y haga clic en Aceptar.

Identity Policy	
FTD-2 Identity Policy	▼
Revert to Defaults	OK Cancel

8. Haga clic en Agregar Regla para crear una nueva regla de ACP. Estos pasos crean una regla para permitir que el usuario dentro del grupo de administradores de AnyConnect se conecte a los dispositivos dentro de la red interna mediante RDP.

Overview Analysis	Policies Dev	ices Objects Al	4P Intelligence				Dep	lay 🧕 8ystem	i Help <del>v</del> admin <del>v</del>		
Access Control > Acc	ess Control Ne	twork Discovery A	pplication Detectors	Correlation Acti	ons 🔻						
Default-Policy Enter Description	Default-Policy You have unsaved changes Analyze Hit Counts Enter Description										
Prefilter Policy: Default P	Prefilter Policy: Default Prefilter Policy: 1000 SSL Policy: None Identity Policy: FID-2 Identity Policy										
	Timberitance Settings   🔣 Policy Assignments (1)										
Rules Security Inte	alligence HTTP Re	sponses Logging	Advanced								
曲 Filter by Device				Show Rule O	onflicts 😣	🔘 Add Category 🛛 🤇	🕽 Add Rule	🚔 Search Rules	×		
a Name :	Sourc Dest Z	Sourc Dest N	VLAN Users	Applic Sourc	Dest P	URLs Sourc	Dest S	Action	e 🖞 🔍 👻		
👻 Mandatory - Defaul	t-Policy (-)										
There are no rules in this	section. Add Rule or A	Add Category									
🛩 Default - Default - Policy (-)											
There are no rules in this	There are no rules in this section. Add Rule or Add Category										
Default Action						Access Control: B	ock All Traffic		× 🔳		

Displaying 0 - 0 of 0 rules  $\ |<\ <\ {\sf Page}\left[ \underline{i} \ \ of\ i\ >\ >|\ C\ |\ {\sf Rules\ per\ page: 100 \ \ } \right.$ 

Especifique un nombre para la regla. Asegúrese de que la regla esté Habilitada y que tenga la Acción apropiada.

En la pestaña Zones, especifique las zonas apropiadas para el tráfico interesante.

El tráfico RDP iniciado por los usuarios entra al FTD originado en la interfaz de la zona exterior y sale de la zona interior.

Add Rule					? ×
Name AC RDP Access		🖌 Enabled	Insert	into Mandatory	
Action 🖌 Allow	V U C	2th 5			
Zones Networks VLAN	Tags Users Application	s Ports URLs	SGT/ISE Attributes	Inspection	Logging Comments
Available Zones C		Source Zone:	s (1)	Destination Zones (1)	)
🔍 side	×	📇 outside-zo	one	🗐 🚑 inside-zone	
🚠 inside-zone	Add to Source Add to Destinat	2 Con			
					Add Cancel

En Redes, defina las redes de origen y de destino.

El objeto AnyConnect\_Pool incluye las direcciones IP asignadas a los clientes de AnyConnect.

El objeto Inside\_Net incluye la subred interna de la red.

Add Ru	le												
Name	AC RDP Access				🖌 Er	nabled		Insert	into Manda	tory			~
Action	Allow			V 🗆 🖉	<b>1</b> 5								
Zone	s Networks VL/	AN Tags Use	rs	Applications	Ports	URLs	SGT/ISE	Attributes			Inspection	Logging	Comments
Availabl	le Networks 🖸		0		Sourc	ce Netwo	rks (1)			Destinati	on Networks	(1)	
🔍 Sear	rch by name or value					Source		Original (	Client	📄 Inside	e_Net		f
	Networks	Geolocation			- A	nyConnec	_Pool		6	_			
Insid	de_Net I-Benchmark-Tests I-Link-Local I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0-12 I-Private-192.168.0.0-16 I-Private-All-RFC1918 i-IPv4-Mapped	6		Add To Source Networks Add to Destination	Enter	r an IP add	Iress		Add	Enter an	IP address		Add
												Add	Cancel

En Usuarios, haga clic en el rango creado anteriormente en Rangos Disponibles, haga clic en el grupo o usuario apropiado en Usuarios Disponibles, luego haga clic en Agregar a Regla.

Si no hay usuarios o grupos disponibles en la sección Usuarios Disponibles, asegúrese de que FMC descargó los Usuarios y los Grupos en la sección de rango y de que se incluyen los Grupos/Usuarios adecuados.

El usuario/grupo especificado aquí se comprueba desde la perspectiva de origen.

Por ejemplo, con lo que se ha definido hasta ahora en esta regla, el FTD evalúa que el tráfico se origina en la zona exterior y se destina a la zona interior, se origina en la red en el objeto AnyConnect\_Pools y se destina a la red en el objeto Inside\_Net, y el tráfico se origina en un usuario del grupo de administradores de AnyConnect.

Add Rule		? >
Name AC RDP Access	Enabled	Insert into Mandatory
Action 🖌 Allow	▼ ¢ D A A I	
Zones Networks VLAN Tags Users	Applications Ports URLs SGT/IS	E Attributes Inspection Logging Comments
Available Realms 🗯	Available Users 🖸	Selected Users (1)
Search by name or value	🔍 Search by name or value	🛃 LAB-AD/AnyConnect Admins 📋
() Special Identities	IAB-AD/*	
📵 LAB-AD	📣 Any Connect Admins	
	AnyConnect Users	
	a it.admin	Add to Rule
	a test.user	
		Add Cancel

En Puertos, se crearon y agregaron objetos RDP personalizados para permitir el puerto TCP y UDP 3389. Observe que RDP podría haber sido agregado bajo la sección Aplicaciones, pero por simplicidad, sólo se verifican los puertos.

Name	AC RDP Access				🖌 E	nabled	Ins	ert into Manda	story 💙			
Action	Allow			• • • •	8 to 5							
Zones	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attribut	85		Inspection	Logging	Comments
vailable	e Ports 🖸		0		Selec	ted Sour	rce Ports (0)		Selected	Destination I	Ports (2)	
🔓 Sean	ch by name or va	lue			any				JP RDP-1	СР		
AOL									🎤 RDP-U	JDP		
Bitto	rrent		^									
P DNS	_over_TCP			Add to								
P DNS	_over_UDP			Source								
FMC-	HTTPS			Add to Destination								
FMC-	-SSH											
P FTD-	3-FDM											
P FTD-	3-SSH											
🖗 FTP												
🖗 нтте	,		*						Protocol 1	TCP (6)	<ul> <li>Port</li> </ul>	Enter a Ad

Por último, asegúrese de que en Registro, Registro al final de la conexión se verifique más adelante para obtener una verificación adicional. Haga clic en Agregar cuando haya terminado.

Add Rule



9. Se crea una regla adicional para el acceso HTTP a fin de permitir a los usuarios del grupo AnyConnect User el acceso al sitio web de Windows Server IIS. Click Save.

Overview Analysis Policies	Devices Objec	ts AMP Intell	gence				Deplo	y 0, System	Help 🔻 admin 🔻
Access Control + Access Control	Network Discove	ary Application D	etectors Cor	relation Actions •					
Default-Policy						You have und	aved changes Analy	ize Hit Counts 📔 S	iave 🔀 Cancel
Prefilter Policy: Default Prefilter Policy			SSL Polic	ty: None		Ident	ity Policy: <u>PTD-2 Iden</u>	tity Policy	
							Te Inhe	ritance Settings   🥂 Po	licy Assignments (1)
Rules Security Intelligence HTT	P Responses Lo	ogging Advanced							
曲 Filter by Device				Show i	Rule Conflicts 😣	Add Category	y 🔾 Add Rule	Search Rules	×
a Name Source Zo	Dest Zones	Source Networks	Dest Netwo	V., Users	A S	Dest Ports	U S D Ac	tion 😈 🐚 🔏	to 🕘 🔍
👻 Mandatory - Default-Policy (1-2)									
1 AC RDP Access 🗠 outside-zone	🗄 inside-zone	AnyConnect_Pool	😹 Inside_Net	Arg 💣 LAB-AD/AnyConnect A	Admins Any A	V PROP-TCP	Any Any Any 🚽	Allow U D .81	5 🛛 • 🖉 6
2 AC HTTP Access du outside-zone	di inside-zone	AnyConnect_Pool	👼 Inside_Net	Are 🧟 LAB-AD/AnyConnect (	Isers Any A	🗸 🎤 НТТР	Any Any Any 😽	Allow U D .81	b 🛛 o 🖉 🖯
🐨 Default - Default-Policy (-)									
There are no rules in this section. Add Rul	e or Add Category								
Default Action						Access Con	trol: Block All Traffic		× 📑

Displaying 1 - 2 of 2 rules  $|\langle \langle Page | \overline{1}$  of  $1 \rangle > | C |$  Rules per page: 100 \*

Configurar exención de NAT

Si hay reglas NAT que afectan al tráfico de AnyConnect, como las reglas PAT de Internet, es importante configurar reglas de exención NAT para que el tráfico de AnyConnect no se vea afectado por NAT.

1. Vaya a Devices > NAT.

Overview Analysis	s Polici	es Devi	ces	Objects AMP In	telligence			Deploy	) <b>Q</b>	System	Help 🔻	admin v
Device Management	NAT	VPN *	QoS	Platform Settings	FlexConfig	Certificates						

Seleccione la política NAT aplicada al FTD.

? X

Overview Analysis	Policies De	vices	Objects   /	AMP Int	telligence		(	Deploy	0,	System	Help 🔻	admin 🔻
Device Management	NAT VPN *	QoS	Platform	Settings	FlexConfig	Certificates						
											🔾 New	Policy
NAT Policy				Dev	vice Type		Status					
FTD-2-NAT-Policy				Thre	at Defense		Targeting 1 devices Up-to-date on all targe	ted devices			<b>P</b> 12	/ 6

2. En esta política NAT, hay una PAT dinámica al final que afecta a todo el tráfico (incluido el tráfico de AnyConnect) que egresa de la interfaz externa a la interfaz externa.

Para evitar que el tráfico de AnyConnect se vea afectado por NAT, haga clic en Agregar regla.

Overview A	nalysis	Policies Devi	ces Objects	AMP Int	telligence				Deploy 🔒	System H	ielp 🔻	admin v
Device Manage	ement	NAT VPN *	QoS Platfor	m Settings	FlexConfig	Certificates						
FTD-2-NA	AT-Poli	cy							🛕 Show Warnin	gs 📔 Sa	sve	😫 Cancel
Rules										E, F	Policy As	signments (1)
A Filter by Device											0	Add Rule
					Original Pack	et	$\sim$	Translated Pac	:ket			
# Direction	Туре	Source Interface Object	Destination Interface Object	Original Sources	Original Destinatio	Orig Ins Serv	Translated	Translated Destination	s Services	Options		
▼ NAT Rules Befo	me											
<ul> <li>Auto NAT Rules</li> </ul>	5											
÷ +	Dynamic	🍓 any	📇 outside-zone	🚌 obj-any			🥵 Interfac	e		🥵 Dns:fa	lse	/ 🛙
▼ NAT Rules After	r											
						Displa	ying 1-1 of 1 row	s K < Page 1	of 1 > >	C Row	s per pa	ge: 100 •

3. Configure una regla de exención de NAT, asegúrese de que la regla sea una regla de NAT manual con tipo estático. Esta es una regla NAT bidireccional que se aplica al tráfico de AnyConnect.

Con esta configuración, cuando el FTD detecta tráfico originado en Inside\_Net y destinado a la dirección IP de AnyConnect (definida por AnyConnect\_Pool), el origen se traduce al mismo valor (Inside\_Net) y el destino se traduce al mismo valor (AnyConnect\_Pool) cuando el tráfico ingresa en inside\_zone y egresa de outside\_zone. Básicamente, esto omite la NAT cuando se cumplen estas condiciones.

							? ×
NAT Rule:	Manual NAT Rul	e v	Insert	:	In Category	▼ NAT Rules Before ▼	
Type:	Static	*	Enable Enable				
Description:							$\bigcirc$
Interface Objects	Translation	PAT Pool	Advanced				
Available Interface O	bjects C		Sour	rce Int	erface Objects (1)	Destination Interface Objects (1)	
🔍 zone		×	i i i	nside-z	one 📋	📸 outside-zone	1
📩 inside-zone							
outside-zone		A	dd to ource				
			dd to				
		Des	tination				
						OK C	Tancel
						UN Y	Control
Add NAT Rule							
							? ×
NAT Rule:	Manual NAT Rul	e 👻	Insert	:	In Category	V NAT Rules Before	? ×
NAT Rule: Type:	Manual NAT Rul	e v	Insert	:	In Category	V NAT Rules Before	? ×
NAT Rule: Type: Description:	Manual NAT Rul Static	e v	Insert Enable	:	In Category	▼ NAT Rules Before ▼	? ×
NAT Rule: Type: Description:	Manual NAT Rul Static	e v	Insert	:	In Category	▼ NAT Rules Before ▼	? ×
NAT Rule: Type: Description: Interface Objects	Manual NAT Rul Static Translation	PAT Pool	Insert Enable Advanced	:	In Category	VAT Rules Before	? ×
NAT Rule: Type: Description: Interface Objects Original Packet	Manual NAT Rul Static Translation	PAT Pool	Insert Enable Advanced	:	In Category Translated Packet	▼ NAT Rules Before ▼	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:*	Manual NAT Rul Static Translation Inside_Net	PAT Pool	Insert Enable	: ]0	In Category Translated Packet Translated Source:	NAT Rules Before     Address	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Net	PAT Pool	Insert: Enable Advanced	: ]@	In Category Translated Packet Translated Source:	NAT Rules Before     Address Inside_Net	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Nel Address	PAT Pool	Insert Enable	]0	In Category In Category Translated Packet Translated Source:	Address	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Nel Address AnyConne	PAT Pool	Insert Enable Advanced	: ]0 ]0	In Category Translated Packet Translated Source: Translated Destination:	NAT Rules Before     Address     Inside_Net     AnyConnect_Pool	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port:	Manual NAT Rul Static Translation Inside_Nel Address AnyConne	PAT Pool t t	Insert Enable	]0	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port:	NAT Rules Before     Address Inside_Net AnyConnect_Pool	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port:	Manual NAT Rul Static Translation Inside_Net Address AnyConne	PAT Pool	Insert Enable	]0	In Category Translated Packet Translated Source: Translated Destination: Translated Source Port:	NAT Rules Before       Address       Inside_Net       AnyConnect_Pool	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination P	Manual NAT Rul Static Translation Inside_Net Address AnyConne	PAT Pool	Insert Enable	]0 ]0 ]0	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	NAT Rules Before       Address       Inside_Net       AnyConnect_Pool	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Destination P	Manual NAT Rul Static Translation Inside_Nel Address AnyConne	PAT Pool	Insert Enable	]0 ]0 ]0	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	NAT Rules Before       Address       Inside_Net       AnyConnect_Pool	? ×
NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination P	Manual NAT Rul Static Translation Inside_Net Address AnyConne	PAT Pool	Insert Enable	]0	In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	NAT Rules Before     Address Inside_Net AnyConnect_Pool	? ×

Además, el FTD está configurado para realizar una búsqueda de ruta en este tráfico y no en el ARP proxy. Haga clic en Aceptar cuando haya terminado.

Add NAT Rule							? ×
NAT Rule:	Manual NAT	Rule 🛩	Insert:	In Category	✓ NAT	Rules Before	*
Type:	Static	~	Enable				
Description:							0
Interface Objects	Translation	PAT Pool	Advanced				
Translate DNS repl	ies that match th	is rule					
Fallthrough to Inter	rface PAT(Destin	ation Interface	)				
IPv6							
Net to Net Mapping	1						
🗹 Do not proxy ARP o	on Destination In	terface					
Perform Route Look	kup for Destination	on Interface					
Unidirectional							
						OK	Cancel

# 4. Haga clic en Guardar.

-	Overview A	nalysis	Policies	Devi	ces Objec	ts AMP	Intelligence			(	Deploy 🔒	System Help	≠ admin <del>v</del>
- 1	Device Manage	ment	NAT	VPN *	QoS PI	latform Settin	gs FlexConfig	Certificates					
F	TD-2-NA	T-Poli	су						You hav	e unsaved changes	🛕 Show Warnin	gs 🔚 Save	Cancel
R	tules											Relicy	Assignments (1)
æ	Filter by Device											0	Add Rule
							Original Pac	:ket	$\sim$	Translated Pack	et		
*	Direction	Туре	Source	e ace Objer	Destination Interface Of	Origina bject Source	l Original Destinat	Orig. ions Servi	Translated	Translated Destinations	Trans Services	Options	
٠	NAT Rules Befo	re											
1	42	Static	🖧 insi	ide-zone	📩 outside-z	one 🚊 Insia	le_Net 📑 AnyCo	snnect_Pool	📻 Inside_N	et 📻 AnyConnec	t_Pool	🍓 Dns:false 🍓 route-looku 🍓 no-proxy-ar	/ 🗊
٠	Auto NAT Rules												
=	+	Dynamic	🥵 any	(	🚠 outside-z	one 🚊 obj-	any		🍓 Interface			🍓 Dns:false	/ 6
۳	NAT Rules After												
								Display	ing 1-2 of 2 rows	IC C Page 1	of 1 > >	C Rows per	page: 100 •

# Implementación

1. Una vez finalizada la configuración, haga clic en Deploy.



2. Haga clic en la casilla de verificación junto al FTD al que se le aplica la configuración y, a continuación, haga clic en Desplegar.

V Device	Inspect Interruption	Туре	Group	Current Version	-
B FTD-2	No	FTD		2020-05-04 09:16 AM	
Selected devices: 1					
				Deploy	ancei
/erificación					
onfiguración final					
onfiguración AAA					
show running-configuration aaa-server aa-server LAB-AD protocol ldap nax-failed-attempts 4	r				
realm-id 5 aa-server LAB-AD host win2016.example server-port 389	. Com				
dap-base-dn DC=example,DC=com dap-group-base-dn DC=example,DC=com					
dap-scope subtree dap-naming-attribute samaccountname dap-login-password *****					
aap-login-an ttd.admin@example.com					

```
> show running-config webvpn
webvpn
 enable Outside
anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
anyconnect profiles Lab disk0:/csm/lab.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 no disable
error-recovery disable
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
group-alias General enable
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
 user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
 http-comp none
 activex-relay disable
 file-entry disable
 file-browsing disable
 url-entry disable
 deny-message none
 anyconnect ssl df-bit-ignore enable
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

Conexión con AnyConnect y verificación de las reglas de la política de control de acceso

S Cisco AnyConnect Secure Mobility Client − □ ×
VPN:         Contacting ftd2.example.com.         ftd2.example.com         ftd2.example.com
Cisco AnyConnect   ftd2.example.com
Username: it.admin
Password: ******
OK Cancel
🕙 Cisco AnyConnect Secure Mobility Client — 🔲 🗙
VPN:         Connected to ftd2.example.com.         ftd2.example.com       Disconnect
00:00:12 IPv4
<b>¢</b> (i)

El usuario IT Admin pertenece al grupo AnyConnect Admins que tiene acceso RDP a Windows Server. Sin embargo, no tiene acceso a HTTP.

Al abrir una sesión de RDP y Firefox en este servidor, se comprueba que este usuario solo puede acceder al servidor a través de RDP.



Si ha iniciado sesión con un usuario de prueba que pertenece al grupo Usuarios de AnyConnect que tiene acceso HTTP pero no acceso RDP, puede comprobar que las reglas de la directiva de control de acceso están surtiendo efecto.



Verificar con eventos de conexión FMC

Dado que el registro estaba habilitado en las reglas de la política de control de acceso, se pueden verificar los eventos de conexión para cualquier tráfico que coincida con esas reglas.

Vaya a Análisis > Conexiones > Eventos.

Overview Analys	sis Policies Devices Obj	ects AMP	Intellige	ence		Deploy 🧕 🧕	System Help 🔻	admin 🔻
Context Explorer	Connections   Intrusions	Files 🔻	Hosts 🔻	Users V	Correlation <b>v</b>	Advanced	<ul> <li>Search</li> </ul>	
Events								
	Security Intelligence Events							

En la Vista de tabla de eventos de conexión, los registros se filtran para mostrar solamente los eventos de conexión para el administrador de TI.

Aquí puede verificar que se permite el tráfico RDP al servidor (TCP y UDP 3389); sin embargo, el tráfico del puerto 80 está bloqueado.

Ove	rview	Analysi	s Policies I	Devices	Objects	AMP II	ntelligence			Depl	oy 🔒 System	n Help <del>v</del> admin <del>v</del>
Cont	ext E	plorer C	onnections > E	vents	Intrusions	<ul> <li>Files</li> </ul>	<ul> <li>Hosts </li> </ul>	Users v	Correlation	<ul> <li>Advanced •</li> </ul>	Search	
									Bookmark This	Page Report Designe	r Dashboard View	Bookmarks Search •
Co	nne	ction Ev	ents (switch	workflow)								
Conn	ections	with Applicati	ion Details > Tab	le View of	f Connection	Events				202	0-05-05 14:14:17 -	Expanding
► Se	arch Co	onstraints ( <u>Edi</u>	t Search Save Sea	erch)								Disabled Columns
Ju	mp to.											
		Action ×	Initiator × IP	Initiato	<u>r User</u> ×		Responder 3	Ingr Secu	ess × rity Zone	Egress × Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code
4		Allow	iii <u>10.10.10.1</u>	📇 <u>it adn</u>	nin (LAB-AD\it	admin, LDA	P) 🗾 <u>192.168.1</u>	1 outsid	e-zone	inside-zone	<u>62473 / tcp</u>	3389 / tcp
4		Block	10.10.10.1	📇 <u>it adn</u>	nin (LAB-AD\it	admin, LDA	P) 🧾 <u>192.168.1</u>	1 outsid	e-zone	inside-zone	62474 / tcp	80 (http) / tcp
4		Block	10.10.10.1	📇 <u>it adn</u>	nin (LAB-AD\it	admin, LDA	P) 👘 <u>192.168.1</u>	1 outsid	e-zone	inside-zone	62475 / tcp	80 (http) / tcp
4		Block	10.10.10.1	📇 it. adn	nin (LAB-AD\it	admin, LDA	P) 👘 <u>192.168.1</u>	1 outsid	e-zone	inside-zone	62476 / tcp	80 (http) / tcp

Para el usuario Test User, puede verificar que el tráfico RDP al servidor esté bloqueado y que el tráfico del puerto 80 esté permitido.

Overvi	ew Analys	is Policies	Devices Objects AMi	P Intelligence		Deplo	γ 🔍 System	Help 🔻 admin 🔻
Context	Explorer	Connections • I	Events Intrusions •	Files • Hosts •	Users   Correlation	<ul> <li>Advanced •</li> </ul>	Search	
					Bookmark This	Page Report Designer	Dashboard View Bo	okmarks Search •
Conr	nection E	vents (switch	workflow)					
Connect	ions with Applic	ation Details > Tab	ele View of Connection Events	E		1 202	)-05-05 14:14:17 - 20	Expanding
Search	n Constraints (E	dit Search Save Se	arch)					Disabled Columns
Jump	to 🔻							
	Action ×	Initiator × IP	Initiator User ×	Responder 3	Security Zone	Egress × Security Zone	Source Port / × ICMP Type	Destination Port / > ICMP Code
4 [	Block	<u>iii 10.10.10.1</u>	📇 test user (LAB-AD\test.use	er, LDAP) 👘 <u>192.168.1</u>	1 outside-zone	inside-zone	<u>62493 / tcp</u>	3389 / top
4	Allow	<u> 10.10.10.1</u>	📇 test user (LAB-AD\test.use	er. LDAP) 👘 192.168.1	1 outside-zone	inside-zone	<u>62494 / tcp</u>	80 (http) / tcp

# Troubleshoot

# Depuraciones

Esta depuración se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la autenticación LDAP: debug Idap 255.

Para resolver problemas de la política de control de acceso de la identidad del usuario, system support firewall-engine-debug se puede ejecutar en clish para determinar por qué se permite o bloquea el tráfico inesperadamente.

Depuraciones de LDAP en funcionamiento

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
```

```
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter = [sAMAccountName=it.admin]
                = [SUBTREE]
        Scope
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
       objectClass: value = top
[53]
[53]
        objectClass: value = person
[53]
        objectClass: value = organizationalPerson
[53]
        objectClass: value = user
[53]
        cn: value = IT Admin
        sn: value = Admin
[53]
[53]
        givenName: value = IT
[53]
        distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]
        instanceType: value = 4
[53]
        whenCreated: value = 20200421025811.0Z
        whenChanged: value = 20200421204622.0Z
[53]
[53]
        displayName: value = IT Admin
[53]
        uSNCreated: value = 25896
[53]
        memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]
        uSNChanged: value = 26119
[53]
        name: value = IT Admin
[53]
        objectGUID: value = &...J..O..2w...c
[53]
        userAccountControl: value = 512
[53]
        badPwdCount: value = 6
[53]
        codePage: value = 0
[53]
        countryCode: value = 0
[53]
        badPasswordTime: value = 132320354378176394
[53]
        lastLogoff: value = 0
[53]
        lastLogon: value = 0
[53]
        pwdLastSet: value = 132319114917186142
[53]
        primaryGroupID: value = 513
        objectSid: value = .....{I...;....j...
[53]
        accountExpires: value = 9223372036854775807
[53]
[53]
        logonCount: value = 0
[53]
        sAMAccountName: value = it.admin
[53]
        sAMAccountType: value = 805306368
[53]
        userPrincipalName: value = it.admin@example.com
[53]
        objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
        dSCorePropagationData: value = 16010101000000.0Z
[53]
[53]
        lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

No se puede establecer una conexión con el servidor LDAP

<#root>

[-2147483611] Session Start

```
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611]
Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Soluciones potenciales:

- Verifique el ruteo y asegúrese de que el FTD esté recibiendo una respuesta del servidor LDAP.
- Si se utiliza LDAPS o STARTTLS, asegúrese de que el certificado de CA raíz correcto sea de confianza para que el intercambio de señales SSL pueda completarse correctamente.
- Verifique que se utilicen la dirección IP y el puerto correctos. Si se utiliza un nombre de host, verifique que DNS pueda resolverlo a la dirección IP correcta.

Enlace DN de inicio de sesión o contraseña incorrecta

#### <#root>

```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid credentials
[-2147483615]
Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Solución potencial: compruebe que el DN de inicio de sesión y la contraseña de inicio de sesión estén configurados correctamente. Esto se puede verificar en el servidor de AD con ldp.exe. Para verificar que una cuenta puede enlazar con éxito usando ldp, siga estos pasos:

1. En el servidor de AD, presione Win+R y busque ldp.exe



2. En Conexión, seleccione Conectar.

Connection       Browse       View       Options       Utilities       Help         Bind       Ctrl+B       Disconnect       Image: Connect and the second and	🚰 Ldp								—		$\times$
ConnectBindCtrl+ BDisconnectNewCtrl+ NSaveSave AsExit	Connection	Browse	View	Options	Utilities	Help	 				
New Ctrl+N Save Save As Exit	Connee Bind Discon	nect	Ctrl+B								
Exit	New Save Save As	5	Ctrl+N								
	Exit										
NUM										NUM	

3. Especifique localhost para el servidor y el puerto adecuado y, a continuación, haga clic en Aceptar.



4. La columna derecha muestra texto que indica una conexión correcta. Vaya a Conexión > Enlazar.

Idap://win2016.exam	com/DC=example,DC	C=com	- [	_ >	×
Connection Browse V	w Options Utilities	Help			
Connection Browse V Connect Bind Cr Disconnect New Ct Save Save As Exit	<ul> <li>Options Utilities</li> <li>Id = Idap_op Established</li> <li>Retrieving b Getting 1 er Dn: (RootD configu CN: current Tim defautti dnsHos domaini dsServ Set Firs Nar cor forestF highest isGloba</li> </ul>	Help pen("localhost", 389); connection to localhost. pase DSA information htries: <b>SE)</b> irationNamingContext: =Configuration,DC=examp Time: 5/1/2020 4:16:55 PM re; NamingContext: DC=examp etName: win2016.example. ControllerFunctionality: 7 = Functionality: 7 = (WIN2016; iceName: CN=NTDS ttings,CN=WIN2016;CN=Se st-Site- me,CN=Sites,CN=Configura m; unctionality: 7 = (WIN2016; CommittedUSN: 13410; iCatalogReady: TRUE;	le,DC=com; I Eastern Da ple,DC=com; .com; • ( WIN2016 I6 ); •rvers,CN=D ation,DC=ex 6 );	vylight ; ); efault- ample,DC	-
	IdanSer	rviceName: example com:	win2016		¥

5. Seleccione Simple Bind y especifique el usuario de cuenta de directorio y la contraseña. Click OK.

# Bind



Х

Con un enlace exitoso, Idp muestra Authenticated as: DOMAIN\username

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		$\times$	
Connection	Browse	View	Options	Utilities	Help					
1.2.840.113556.1.4.2255;         1.2.840.113556.1.4.2256;         1.2.840.113556.1.4.2309;         supportedLDAPPolicies (20): MaxPoolThreads;         MaxPercentDirSyncRequests; MaxDatagramRe         MaxReceiveBuffer; InitRecvTimeout;         MaxConnections; MaxConnkleTime; MaxPageS         MaxBatchReturnMessages; MaxQueryDuration         MaxDirSyncDuration; MaxTempTableSize;         MaxResultSetSize; MinResultSets;         MaxResultSetSize; MinResultSets;         MaxResultSetSize; MaxNotificationPerCon         MaxValRange; MaxValRangeTransitive;         ThreadMemoryLimit; SystemMemoryLimitPercer         supportedLDAPVersion (2): 3; 2;         supportedSASLMechanisms (4): GSSAPI; GSS-         SPNEGO; EXTERNAL; DIGEST-MD5;         Tes = Idap_simple_bind_s(Id, 'ftd.admin@example.com', <unavailable>); // v.3         Authenticated as: 'EXAMPLEDEdd admin'</unavailable>							cv; ize; ; n; it;	^		
			<	unavailable	<pre>&gt;); // v.3 ed as: 'EXAl</pre>	_s(id, itd.ddi	nin'.	npic.com,		
			-						'	¥
Ready										

Si se intenta enlazar con un nombre de usuario o una contraseña no válidos, se producirá un error como los dos que se muestran aquí.

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com	_		×	
Connection	Browse	View	Options	Utilities	Help				
				Max Max Max Thre supporte supporte SPN es = Idap_s unavailable suthenticate es = Idap_s unavailable	ResultSetSize (ResultSetSize (ValRange; Ma eadMemoryLin edLDAPVersid edSASLMech IEGO; EXTERN simple_bind_si ed as: "EXAMP simple_bind_si e>); // v.3	e; MinResul rConn; Max axValRange nit; Systemi on (2): 3; 2; anisms (4): NAL; DIGES (Id, 'ftd.adm PLE\ftd.adm (Id, 'wrong)	tSets; Notificati Transitiv MemoryLi GSSAPI; T-MD5; in@exan in". @exampl	ionPerConn 'e; imitPercent ; GSS- nple.com', e.com',	
			< E S C E ir	unavailable rror <49>: I server error comment: Ac rror 0x8009 ivalid	<pre>&gt;&gt;); // V.3 Idap_simple_b r: 80090308: L cceptSecurity 90308 The tok</pre>	ind_s() fail .dapErr: DS Context err en supplied	ed: Invalia ID-0C090 or, data d to the fu	d Credentia )42A, 52e, v3839 unction is	ls V
Ready									

El servidor LDAP no puede encontrar el nombre de usuario

#### <#root>

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter = [samaccountname=it.admi]
        Scope
               = [SUBTREE]
[-2147483612]
Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
```

[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1

Solución potencial: compruebe que AD puede encontrar el usuario con la búsqueda realizada por el FTD. Esto se puede hacer con ldp.exe también.

1. Después de enlazar correctamente como se ve arriba, navegue hasta Ver > Árbol.

Connection       Browse       View       Options       Utilities       Help         Tree       Ctrl+T       Interprise Configuration       //axPoolThreads; sts; MaxDatagramRecv; vTimeout; nkleTime; MaxPageSize; s; MaxQueryDuration;       *         Status Bar       vTimeout; nkleTime; MaxPageSize; s; MaxQueryDuration;       *         Set Font       MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets;       MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;         Terme       res = Idap_simple_bind_s(Id, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'.</unavailable>	🔝 Idap://w	in2016.exa	mple.	com/DC=e	xample,DC:	=com			_		×	<
Tree       Ctrl+T         Enterprise Configuration       MaxPoolThreads; sts; MaxDatagramRecv; vTimeout; nldleTime; MaxPageSize; s; MaxQueryDuration; MaxCeryDuration; MaxTempTableSize; MaxResutSetSize; MinResutSets; MaxResutSetSize; MinResutSets; MaxResutSetSize; M	Connection	Browse	View	Options	Utilities	Help						
<pre>introdumentoryLinit, SystemmentoryLinit erectit, supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;</pre>		browse	✓	Tree Enterprise Status Bar Set Font	Configurati Max Max Max Max Thre	Ctrl+T Duration; Ma etSize; MinF etsPerConn ge; MaxValF prod. imit: System	/lax sts cvT nkt s; I axTer Result ; Max Range stem	xPoolThr s; MaxDa Timeout; IleTime; I MaxQuei mpTable tSets; tSets; tSets; tSets; tSets; tSets; tSets; tSets;	eads; atagramR MaxPage ryDuratio Size; ionPerCo /e; imitPerce	ecv; Size; n; onn;	^	
					supporte supporte SPN 	imple_bi >); // v.3	version (2): Mechanisms (TERNAL; D nd_s(Id, 'ftd ) XAMPLE\ftd	: 3; 2; s (4): IGES I.adm	in'.	; GSS-	/,	*

2. Especifique el DN base configurado en el FTD y haga clic en Aceptar

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	ОК

3. Haga clic con el botón derecho en el DN base y luego haga clic en Buscar.

🔐 Idap://win2	2016.exa	mple.co	om/DC=ex	=com	- 🗆 ×	2								
Connection E	Browse	View	Options	Utilities	Help									
DC=exampl	le,DC=co	om	Search Virtual L Delete Modify Modify Add chil Compar Advance	ist View DN d e	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com;	^							
									Copy C Copy Select Clear o	Copy Copy Select al Clear ou	N I tput	Ctrl+C Ctrl+N	311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new do	cument													

4. Especifique los mismos valores DN base, Filtro y Ámbito que se ven en las depuraciones.

En este ejemplo, estos son:

- DN base: dc=ejemplo,dc=com
- Filtro: samaccount=it.admi
- Ámbito:SUBÁRBOL

🔐 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 X									
Connection	Browse View Options Utilities Help										
Search	×	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^								
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C									
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:0									
Scope O Base	One Level Subtree	lers,DC=example,DC=com; \$8811D1ADED00C04FD8D5CD:C example,DC=com;									
Attributes:	objectClass;name;description;canonicalName ~	68811D1ADED00C04FD8D5CD:C mple,DC=com;									
Options	Run Close	2020 3:43:59 PM Eastern Daylight									
	***Searching kdap_search_s(kd, "DC=0 "sAMAccountName=it.ad Getting 0 entries:	example,DC=com", 2, dmi", attrList, 0, &msg)	~								
Ready	eady										

ldp encuentra 0 entradas porque no hay ninguna cuenta de usuario con el sAMAccountname it.admi bajo el DN base dc=example,dc=com.

Otro intento con el sAMAccountname it.admin correcto muestra un resultado diferente. Idp encuentra 1 entrada bajo el DN base dc=example,dc=com e imprime ese DN de usuario.

🔝 Idap://wi	n2016.example	com/DC=e	ample,DC	=com		>	~
Connection	Browse View	Options	Utilities	Help			
Search					$\times$	58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base DN:	DC=example,D	C=com			$\overline{}$	58811D1ADED00C04FD8D5CD:C ample,DC=com;	•
 Filter:	sAMAccountNar	ne=it.admin			$\overline{}$	D211D1AA4B00C04FD7D83A:C lers,DC=example,DC=com;	)
Scope	O <u>O</u> ne Level	<u> ◎</u> <u>S</u> ubtre	e			58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C nole DC=com;	2
<u>A</u> ttributes:	objectClass;nar	ne;description	n;canonicalN	Name	$\sim$	020 3:43:59 PM Eastern Dayligh	t
Options		<u>R</u> un	1	<u>C</u> lose		)20 2:41:57 PM Eastern Daylight	
		- * () () () ()	***Searching dap_search sAMAccour Getting 1 en On: CN=IT A canonic name: IT objectCl use	) s(Id, "I ntName: tries: A <b>dmin,(</b> alName: Admin; ass (4): r;	DC=e =it.ad CN=U : exar ; : top;	example,DC=com", 2, Imin", attrList, 0, &msg) <b>Jsers,DC=example,DC=com</b> mple.com/Users/IT Admin; person; organizationalPerson;	~
Ready							

Contraseña incorrecta para el nombre de usuario

## <#root>

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter = [samaccountname=it.admin]
        Scope
               = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
```

```
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
[-2147483613]
Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext erro
[-2147483613]
Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Posible solución: compruebe que la contraseña de usuario está configurada correctamente y que no ha caducado. Al igual que el DN de inicio de sesión, el FTD realiza un enlace con AD con las credenciales del usuario.

Este enlace también se puede hacer en ldp para verificar que AD pueda reconocer las mismas credenciales de nombre de usuario y contraseña. Los pasos en ldp se muestran en la sección DN de Login de Enlace y/o contraseña incorrecta.

Además, los registros del Visor de eventos de Microsoft Server se pueden revisar por un motivo de error potencial.

# Prueba AAA

El comando test aaa-server se puede utilizar para simular un intento de autenticación del FTD con un nombre de usuario y una contraseña específicos. Esto se puede utilizar para probar fallos de conexión o autenticación. El comando es test aaa-server authentication [AAA-server] host [AD IP/hostname].

```
<#root>
```

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
realm-id 7
aaa-server
LAB-AD
host
win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
> test aaa-server authentication
```
LAB-AD

host

win2016.example.com

```
Username: it.admin
Password: *******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

## Capturas de paquetes

Las capturas de paquetes se pueden usar para verificar la disponibilidad al servidor AD. Si los paquetes LDAP dejan el FTD, pero no hay respuesta, esto podría indicar un problema de ruteo.

La captura muestra el tráfico LDAP bidireccional.

```
> show route 192.168.1.1
Routing entry for 192.168.1.0 255.255.255.0
 Known via "connected", distance 0, metric 0 (connected, via interface)
 Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
 match tcp any host 192.168.1.1 eq ldap
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password ******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
 match tcp any host 192.168.1.1 eq ldap
> show capture AD
54 packets captured
   1: 23:02:16.770712
                            192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768
                            192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
   2: 23:02:16.772009
   3: 23:02:16.772039
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
                            192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
   4: 23:02:16.772482
   5: 23:02:16.772924
                            192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
   6: 23:02:16.772955
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
   7: 23:02:16.773428
                            192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
   8: 23:02:16.775030
                            192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
   9: 23:02:16.775075
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
[...]
```

```
54 packets shown
```

## Registros del Visor de sucesos de Windows Server

Los registros del Visor de eventos en el servidor de AD pueden proporcionar información más detallada sobre el motivo de un error.

1. Busque y abra el Visor de sucesos.



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).