Configuración de Firepower Management Center y FTD con LDAP para autenticación externa

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Diagrama de la red
Configurar
Configuración básica de LDAP en la GUI de FMC
Acceso al shell para usuarios externos
Autenticación externa a FTD
Funciones de usuario
<u>SSL o TLS</u>
Verificación
Base de búsqueda de pruebas
Probar integración LDAP
Troubleshoot
¿Cómo interactúan FMC/FTD y LDAP para descargar usuarios?
¿Cómo interactúan FMC/FTD y LDAP para autenticar una solicitud de inicio de sesión de un usuario?
SSL o TLS no funcionan como se esperaba
Información Relacionada

Introducción

Este documento describe cómo habilitar la autenticación externa del protocolo ligero de acceso a directorios (LDAP) de Microsoft con Cisco Firepower Management Center (FMC) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FTD de Cisco
- Cisco FMC
- LDAP de Microsoft

Componentes Utilizados

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

- FTD 6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

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

El FMC y los dispositivos gestionados incluyen una cuenta de administración predeterminada para el acceso a la gestión. Puede agregar cuentas de usuario personalizadas en el FMC y en dispositivos administrados, ya sea como usuarios internos o, si se admite para su modelo, como usuarios externos en un servidor LDAP o RADIUS. La autenticación de usuario externo es compatible con FMC y FTD.

 \cdot Usuario interno: el dispositivo FMC/FTD comprueba una base de datos local para la autenticación del usuario.

· Usuario externo: Si el usuario no está presente en la base de datos local, la información del sistema de un servidor de autenticación LDAP o RADIUS externo rellena su base de datos de usuarios.

Diagrama de la red



Configurar

Configuración básica de LDAP en la GUI de FMC

Paso 1. Desplácese hasta System > Users > External Authentication:

← → C ▲ Not secure 192.0.2.5/ddd/#ExternalAuthentication	1 x \varTheta 🗄
Overview Analysis Policies Devices Objects AMP Intelligence	Deploy 🧕 System Help 🔹 admin 🗸
3	Configuration Users Domains Integration Updates Licenses Health Monitoring Tools
Users User Roles External Authentication	2.
	🔚 Save 😫 Cancel 🖌 Save and Apply
Default User Role: None Shell Authentication Disabled *	Add External Authentication Object
Name	Hethod Enabled





Paso 3. Complete los campos obligatorios:

External Authentication Object	:	
Authentication Method	LDAP V	
CAC	Use for CAC authentication and authorization	
Name *	SEC-LDAP Name the Extern	al Authentication Object
Description		
Server Type	MS Active Directory Set Defaults Choose MS Active	e Directory and click 'Set Defaults'
Primary Server		
Host Name/IP Address *	192.0.2.10	ex. IP or hostname
Port *	Default port is 38	9 or 636 for SSL
Backup Server (Optional)		
Host Name/IP Address		ev. IP or hostname
Port	290	EAL IF OF INSUMINE
	507	
LDAP-Specific Parameters	*Base DN specifies where users will be fou	ind
Base DN *	DC=SEC-LAB Fetch	DNs ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (lcn=jsmith), (&(cn=jsmith)(l(cn=bsmith)(cn=csmith*)))
User Name *	Administrator@SEC-LAB0	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	Username of LDA	P Server admin
Confirm Password *		
Show Advanced Options	•	
	*Default when 'Set Default	d option is clicked
Attribute Mapping		s option is clicked
UI Access Attribute *	sAMAccountName	Attrs
Shell Access Attribute *	sAMAccountName	

Group Controlled Access Roles (Optional) -

Access Admin		
Administrator		
Discovery Admin		
External Database User		
Intrusion Admin		
Maintenance User		
Network Admin		
Security Analyst		
Security Analyst (Read Only)		
Security Approver		
Threat Intelligence Director (TID) User		
View-Only-User (Read Only)		
Default User Role	Access Admin Administrator Discovery Admin External Database User	To specify the default user role if user is not found in any group
Group Member Attribute	member	
Group Member URL Attribute		
Shell Access Filter	✓ Same as Base Filter	
(Mandatory for FTD devices)		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith
,		
Additional Test Parameters		
User Name		
Password		
*Required Field		
	Save Test Cancel	

Paso 4. Habilite el External Authentication Objeto y guardar:

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	0 Sy	stem Help	admin v
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring	 Tools •
Users User Roles External Authentication								2.	
							🗟 Save 【	Cancel 🗹 S	iave and Apply
Default User Role: None Shell Authentication Disabled •							O Add	External Auther	tication Object
Name							Hethod	Enabled	
1. SEC-LDAP New External Authentication Object							LDAP		060
								1.	3

Acceso al shell para usuarios externos

El FMC admite dos usuarios de administración interna diferentes: uno para la interfaz web y otro con acceso CLI. Esto significa que existe una clara distinción entre los usuarios que pueden acceder a la GUI y los que también pueden acceder a la CLI. En el momento de la instalación, la contraseña para el usuario admin predeterminado se sincroniza para que sea la misma en la GUI y la CLI, sin embargo, son rastreados por diferentes mecanismos internos, y eventualmente pueden ser diferentes.

Los usuarios externos de LDAP también deben tener acceso al shell.

Paso 1. Desplácese hasta System > Users > External Authentication y haga clic en Shell Authentication como se ve en la imagen y guardar:



Paso 2. Implementar cambios en FMC.

Una vez configurado el acceso al shell para usuarios externos, se habilita el inicio de sesión a través de SSH como se ve en la imagen:



Autenticación externa a FTD

La autenticación externa se puede habilitar en FTD.

Paso 1. Desplácese hasta Devices > Platform Settings > External Authentication. Haga clic en Enabled y guarde:

Overview Analysis Policies	Devices Object	ts AMP Intelligence					
Device Management NAT 1.1	/PN V QoS Pla	atform Settings FlexConfig (Certificates				
Platform-Policy	2.						
Enter Description							
ARP Inspection				Manage Exte	rnal Authentication	Server	2
Banner 3.	Name	Description	Hethod	Server:Port	Encryption	Enabled	
External Authentication	SEC-LDAP		LDAP	192.0.2.10:389	no		
Fragment Settings						4.	
HTTP							
Secure Shell							
SMTP Server							
SNMP							
SSL Susion							
Timeouts							
Time Synchronization							
UCAPL/CC Compliance							
	"Applicable on FTD v6.2	.3 and above					

Funciones de usuario

Los privilegios de usuario se basan en la función de usuario asignada. También puede crear roles de usuario personalizados con privilegios de acceso adaptados a las necesidades de su organización o puede utilizar roles predefinidos como Analista de seguridad y Administrador de descubrimiento.

Existen dos tipos de funciones de usuario:

- 1. Funciones de usuario de interfaz web
- 2. Funciones de usuario de CLI

Para obtener una lista completa de funciones predefinidas y más información, consulte; <u>Funciones de usuario</u>.

Para configurar un rol de usuario predeterminado para todos los objetos de autenticación externa, navegue hasta System > Users > External Authentication > Default User Role. Elija la función de usuario predeterminada que desee asignar y haga clic en Save.

Overview Analysis Policies Devices Objects AMP Intelligence								Deploy	0 Syste	m Help +	admin +
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health + I	Monitoring •	Tools •
Users User Roles External Authentication											
								6	Save 🙆 Ca	ncel 📝 Sa	re and Apply
Default User Role: None Shell Authentication Enabled (SEC-LDAP)									O Add Ext	ernal Authenti	cation Object
Name									Hethod	Enabled	
1. SEC-LDAP									LDAP		182
	Default User Role Configuration										
		Administrator External Database User (Read Only)									
		Security Analyst									
	Participation Parlow	Security Approver									
	Default Oser Roles	Access Admin									
		Network Admin Maintenance User									
		Discovery Admin									
	Custom Liser Boles	View-Only-Liter (Read Only) (Clobal									
		Contract (man only) (anota)									
		Sav	Cancel								

Para elegir una función de usuario predeterminada o asignar funciones específicas a usuarios específicos de un grupo de objetos determinado, puede elegir el objeto y desplazarse a Group Controlled Access Roles como se ve en la imagen:

Group Controlled Access Roles	(Optional) •
Access Admin	
Administrator	h.potter@SEC-LAB.
Discovery Admin	
External Database User	s.rogers@SEC-LAB
Intrusion Admin	
Maintenance User	
Network Admin	h.simpson@SEC-LAB
Security Analyst	r.weasley@SEC-LAB
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	
View-Only-User (Read Only)	ma.simpson@SEC-LAB
Default User Role	Access Admin Administrator Discovery Admin External Database User

SSL o TLS

DNS debe configurarse en el FMC. Esto se debe a que el valor de Asunto del Certificado debe coincidir con el Authentication Object Primary Server Hostname. Una vez configurado el LDAP seguro, las capturas de paquetes ya no muestran solicitudes de enlace de texto sin cifrar.

SSL cambia el puerto predeterminado a 636 y TLS lo mantiene como 389.

Nota: el cifrado de TLS requiere un certificado en todas las plataformas. Para SSL, el FTD también requiere un certificado. Para otras plataformas, SSL no requiere un certificado. Sin embargo, se recomienda que siempre cargue un certificado para SSL para evitar ataques de intrusos.

Paso 1. Desplácese hasta Devices > Platform Settings > External Authentication > External Authentication Object e introduzca la información SSL/TLS de Opciones avanzadas:

LDAP-Specific Parameters			
Base DN *	DC=SEC-LAB	Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter			ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB		ex. cn=jsmith,dc=sourcefire,dc=com
Password *			
Confirm Password *			
Show Advanced Options	•		
Encryption	SSL O TLS None		
SSL Certificate Upload Path	Choose File No file chosen		ex. PEM Format (base64 encoded version of DER)
User Name Template	%5		ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30		

Paso 2. Cargue el certificado de la CA que firmó el certificado del servidor. El certificado debe estar en formato PEM.

LDAP-Specific Parameters		
Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB	ex. cn=jsmith,dc=sourcefire,dc=com
Password *		
Confirm Password *		
Show Advanced Options	•	
Encryption	SSL TLS None	
SSL Certificate Upload Path	Choose File CA-Cert-base64.cer	ex. PEM Format (base64 encoded version of DER)
User Name Template	%5	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

Paso 3. Guarde la configuración.

Verificación

Base de búsqueda de pruebas

Abra un símbolo del sistema de Windows o PowerShell donde LDAP esté configurado y escriba el comando: dsquery user -name

Por ejemplo:

.

```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```

Σ	Administrator: Windows PowerShell – 🗖	x	
PS 0 PS 0	C:\Users\Administrator> dsquery user -name harry" +Harry Potter,CN=Users,DC=SEC-LAB C:\Users\Administrator> C:\Users\Administrator> dsquery user -name * Administrator,CN=Users,DC=SEC-LAB =cGuest,CN=Users,DC=SEC-LAB =krbtgt,CN=Users,DC=SEC-LAB =anthony E. Stark,CN=Users,DC=SEC-LAB =br. Robert B. Banner,CN=Users,DC=SEC-LAB =0r. Robert B. Banner,CN=Users,DC=SEC-LAB =finny Weasley,CN=Users,DC=SEC-LAB =harry Potter,CN=Users,DC=SEC-LAB =Harry Potter,CN=Users,DC=SEC-LAB =Hermione Granger,CN=Users,DC=SEC-LAB =lisa Simpson,CN=Users,DC=SEC-LAB =Lisa Simpson,CN=Users,DC=SEC-LAB =Margg Simpson,CN=Users,DC=SEC-LAB =Marge Simpson,CN=Users,DC=SEC-LAB =Neville Longbottom,CN=Users,DC=SEC-LAB =Ron Weasley,CN=Users,DC=SEC-LAB =Steven Rogers,CN=Users,DC=SEC-LAB =Steven Roger		
<	III	> .;	đ

Probar integración LDAP

Desplácese hasta System > Users > External Authentication > External Authentication Object. En la parte inferior de la página, hay un Additional Test Parameters COMO se ve en la imagen:

Additional Test Parameters User Name Password	h.potter
*Required Field	Save Test Cancel

Elija el Test para ver los resultados.

Overview Analysis Policies Devices Objects	AMP Intelligence							Deploy	0
			Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Heal
Users User Roles External Authentication									
		Success Test Complete.	c						
	External Authentication Object								
	Authentication Method LDAP CAC Use for CAC authe	ntication and authorization							
	Name * SEC-LDAP Description								
	Server Type MS Active Directory *	Set Defaults							
	A								

A					Capturing from Ethemeti						
File E	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help										
16 🔳	4000	R 🖸 🧣 🖷	🕾 Ŧ ± 🖬 🔳 🍳 Q	Q. 11							
top.p	ng port399 Ma (p. addr192.0.2.5										
No.	Time	Source	Destination	Protocol	Length Info	~					
17	99 55.131546	192.0.2.5	192.0.2.10	TCP	66 39784 - 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3077124549 TSecr=25708266						
18	00 55.131547	192.0.2.5	192.0.2.10	LDAP	127 bindRequest(1) "CN+Marry Potter,CN+Users,DC+SEC-LAB						
+ 15	01 55.132124	192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success						
14	02 55.132184	192.0.2.5	192.0.2.10	TCP	66 39784 + 389 [ACK] Seq=62 Ack=23 Win=29312 Len=0 TSval=3077124549 TSecr=25708266						
18	03 55.132213	192.0.2.5	192.0.2.10	LDAP	73 unbindRequest(2)						
18	04 55.132213	192.0.2.5	192.0.2.10	TCP	66 39784 → 389 [FIN, ACK] Seq=69 Ack=23 Win=29312 Len=0 TSval=3077124550 TSec==25708266						
18	05 55.132227	192.0.2.10	192.0.2.5	TCP	66 389 = 39784 [ACK] Seq=23 ACK=70 Win=66560 Len=0 TSval=25708266 TSecr=3077124549	×					
D Fra	ne 1800: 127 b	tes on wire (1016	bits), 127 bytes captur	red (1016	bits) on interface \Device\WFF_{77DC31F6-8250-4F19-8412-E4596F960108}, id 0						
₽ Eth	ernet II, Src:	VMware_29:cf:2d (00:0c:29:29:cf:2d), Dst:	: Vhuare_el	b:1d:f7 (00:0c:29:eb:1d:f7)						
▷ Int	ernet Protocol	Version 4, Src: 1	92.0.2.5, Dst: 192.0.2.1	10							
P Tra	nsmission Cont	rol Protocol, Src	Port: 39784, Dst Port: 3	389, Seq: 3	1, Ack: 1, Len: 61						
- L18	htweight Direct	tory Access Protoc	01		* starls						
-	conversage of	iokequest(1) CN+H	arry Potter, chausers, uca	SEC-LAB	single						
	4 protocol0p:	hindRequest (8)									
	4 bindReque	st									
	versio	01.3									
	nme: Childarry Potter, Childers, DCxSIC-LAB										
	# authentication: simple (0)										
	sim	ple: cisco									
	[Response In	: 1801]									

Troubleshoot

¿Cómo interactúan FMC/FTD y LDAP para descargar usuarios?

Para que FMC pueda extraer usuarios de un servidor LDAP de Microsoft, primero debe enviar una solicitud de enlace en el puerto 389 o 636 (SSL) con las credenciales de administrador LDAP. Una vez que el servidor LDAP es capaz de autenticar FMC, responde con un mensaje de éxito. Por último, el CSP puede realizar una solicitud con el mensaje de solicitud de búsqueda que se describe en el diagrama:

<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

Observe que la autenticación envía contraseñas en el modo claro de forma predeterminada:

83	4.751887	192.0.2.5	192.0.2.10	TCP	74 38002 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344 TSecr=0 WS=128						
84	4.751920	192.0.2.10	192.0.2.5	TCP	74 389 → 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=25348746 TSecr=3073529344						
85	4.751966	192.0.2.5	192.0.2.10	TCP	_66 38002 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746						
86	4.751997	192.0.2.5	192.0.2.10	LDAP	110 bindRequest(1) "Administrator@SEC-LAB0" simple						
 87 	4.752536	192.0.2.10	192.0.2.5	LDAP	88 bindResponse(1) success						
88	4.752583	192.0.2.5	192.0.2.10	TCP	66 38002 → 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746						
89	4.752634	192.0.2.5	192.0.2.10	LDAP	122 searchRequest(2) "DC=SEC-LAB ' wholeSubtree						
 Frame Ethern Intern Transm Lightw 	Frame 86: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{77DC31F6-8250-4F19-8412-E4596F960108}, id 0 Ethernet II, Src: Whware_29:cf:2d (00:0c:29:29:cf:2d), Dst: Whware_eb:1d:f7 (00:0c:29:eb:1d:f7) Internet Protocol Version 4, Src: 192.0.2.5, Dst: 192.0.2.10 Transmission Control Protocol, Src Port: 38002, Dst Port: 389, Seq: 1, Ack: 1, Len: 44 Lightweight Directory Access Protocol										
⊿ LDA	PMessage bind	Request(1) "Administr	ator@SEC-LAB0" simple								
	nessageID: 1										
4	protocolOp: b:	indRequest (0)									
	4 bindRequest										
	version:	3									
	name: Ad	ministrator@SEC-LAB0									
	4 authenti	ication: simple (0)									
	simpl	e: Ciscot@c									
	Response In:	871									

¿Cómo interactúan FMC/FTD y LDAP para autenticar una solicitud de inicio de sesión de un usuario?

Para que un usuario pueda iniciar sesión en FMC o FTD mientras esté habilitada la autenticación LDAP, la solicitud de inicio de sesión inicial se envía a Firepower; sin embargo, el nombre de usuario y la contraseña se reenvían a LDAP para obtener una respuesta de denegación/éxito. Esto significa que el FMC y el FTD no mantienen la información de contraseña localmente en la base de datos y, en su lugar, esperan la confirmación de LDAP sobre cómo proceder.





4							*Ethernet1	
File Edi	t View Go Cap	ture Analyze Statistics	Telephony Wireless To	ools Hel	р			
(= 4	🤨 🕘 💄 🔁 🗙	🖸 🍳 🗢 🗢 🗟 🖗	୬ 📃 🗏 €, ୧, ୧,					
tcp.por	t==389 && ip.addr==1	92.0.2.5 && ldap.messageID =	-= 1					
No.	Time	Source	Destination	Protocol	Length	Info		
58	3 13:11:59.695671	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1) '</pre>	"Administrator@SEC-LAB0" simple	
• 59	13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	
67	13:11:59.697773	192.0.2.5	192.0.2.10	LDAP	110	<pre>bindRequest(1) '</pre>	"Administrator@SEC-LAB0" simple	
69	13:11:59.699474	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	
97	13:11:59.729988	192.0.2.5	192.0.2.10	LDAP	127	<pre>bindRequest(1) '</pre>	"CN=Harry Potter, CN=Users, DC=SEC-LAB	" simple
98	3 13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	<pre>bindResponse(1)</pre>	success	

Si se aceptan el nombre de usuario y la contraseña, se agrega una entrada en la GUI web como se ve en la imagen:

Overview Analysis Policies Devices O	bjects AMP Intelligence							Deploy	Ø Syste	m Help 🕶	h.potter +
			Configuration	Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
Users User Roles External Authentication											
										00	reate User
Username	Roles	Authentication Method		Pas	sword Lifetin	ю					
admin	Administrator	Internal		Unli	mited						0
h.cotter	Administrator	External									0
Username admin h.eotter	Roles Administrator Administrator	Adhentication Hethod Internal External		Pas	sword Lifetim	M					1

Ejecute el comando show user en FMC CLISH para verificar la información del usuario: > show user

El comando muestra información de configuración detallada para los usuarios especificados. Se muestran estos valores:

Login: el nombre de inicio de sesión

UID: el ID de usuario numérico

Autenticación (local o remota): cómo se autentica al usuario

Acceso (básico o de configuración): el nivel de privilegio del usuario

Habilitado (habilitado o deshabilitado): indica si el usuario está activo.

Restablecer (Sí o No): indica si el usuario debe cambiar la contraseña la próxima vez que inicie sesión.

Exp (Nunca o un número): el número de días hasta que se debe cambiar la contraseña del usuario

Advertencia (N/D o número): el número de días que se concede a un usuario para cambiar su contraseña antes de que caduque

Str (Sí o No): si la contraseña del usuario debe cumplir los criterios para comprobar la seguridad Bloquear (Sí o No): indica si la cuenta del usuario se ha bloqueado debido a demasiados errores de inicio de sesión.

Max (N/D o un número): el número máximo de inicios de sesión fallidos antes de que se bloquee la cuenta del usuario

SSL o TLS no funcionan como se esperaba

Si no habilita DNS en los FTD, puede ver errores en el registro de conexiones que sugieren que LDAP es inalcanzable:

MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2. MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61

Asegúrese de que Firepower puede resolver el FQDN de servidores LDAP. Si no es así, agregue el DNS correcto tal como se ve en la imagen.

FTD: Acceda a FTD CLISH y ejecute el comando: > configure network dns servers

```
x
₽
                                 192.0.2.6 - PuTTY
root@SEC-FTD:/etc# ping WIN.SEC-LAB
ping: unknown host WIN.SEC-LAB
root@SEC-FTD:/etc# exit
exit
admin@SEC-FTD:/etc$ exit
logout
 configure network dns servers 192.0.2.15
 expert
NOTICE - Shell access will be deprecated in future releases
        and will be replaced with a separate expert mode CLI.
***********************
admin@SEC-FTD:~$ ping WIN.SEC-LAB
PING WIN.SEC-LAB
                  (192.0.2.15) 56(84) bytes of data.
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=1 ttl=128 time=0.176 ms
64 bytes from win.sec-lab.net (192.0.2.15): icmp seq=2 ttl=128 time=0.415 ms
   WIN.SEC-LAB
                  ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms
admin@SEC-FTD:~$
```

FMC: Elegir _{System > Configuration}y, a continuación, seleccione Interfaces de gestión como se muestra en la imagen:

Access List							
Access Control Preferences	• Inter	faces					
Audit Log	Link	Name	Channels	MAC Addres	s	IP	
Audit Log Certificate						Address	
Change Reconciliation	0	eth0	Management Traffi	c 00:0C:29:29	CF:2D	192.0.2.5	0
DNS Cache			Event Traffic				_
Dashboard	• Rout	20					
Database	10000						
Email Notification	IPv4	Routes			_		•
External Database Access	Dest	ination	Netmask	Interface	Gatev	vay	
HTTPS Certificate					192.0	.2.1	6
Information							
Intrusion Policy Preferences	IPv6	Routes					•
Language	Dest	ination	Prefix Length	Interface	Gate	eway	
Login Banner							
Management Interfaces	• Shar	ed Setti	ings				
Network Analysis Policy Preferences	s Hostn	ame	s	EC-FMC			
Process	Doma	ins	-			_	
REST API Preferences	Deirera	N DEC Car				_	
Remote Storage Device	PTIMA	ry Unio Ser	ver 1	92.0.2.10			
SNMP	Secon	dary DNS 5	Server				
Shell Timeout	Tertiar	y DNS Ser	ver				
Time	Remot	e Manager	ment Port 8	305			
Time Synchronization							
UCAPL/CC Compliance	• ICM	2v6					
User Configuration	Allow	Sending Ec	the Reply				
/Mware Tools	Packet	ts		9			
Vulnerability Mapping	Allow	Sending De	estination G				
Web Analytics	Unrea	chable Pad	kets	<i>,</i>			
	• Prox	v					
	Enable	ed)			

Asegúrese de que el certificado cargado en FMC es el certificado de la CA que firmó el certificado de servidor de LDAP, como se muestra en la imagen:



Utilice capturas de paquetes para confirmar que el servidor LDAP envía la información correcta:

							*Ethernet0	
File	Edit View Go	Capture Analyze Sta	tistics Telephony Wireles	s Tools H	elp			
	🔳 🔬 💿 🌗 📇	🗙 🖸 🔍 🗢 🖻	i T 🕹 🖬 🗐 Q Q	Q. II				
	lap tis && ip.addr==1	92.0.2.5						
No.	Time	Source	Destination	Protocol	Length Info			
	3 0.143722	192.0.2.5	192.0.2.15	TLSv1.2	107 Application Data			
	4 0.143905	192.0.2.15	192.0.2.5	TLSv1.2	123 Application Data			
	22 2.720710	192.0.2.15	192.0.2.5	TLSv1.2	1211 Application Data			
	29 3.056497	192.0.2.5	192.0.2.15	LDAP	97 extendedReq(1) LDAP_START_TLS_C	DID		
Ш.	30 3.056605	192.0.2.15	192.0.2.5	LDAP	112 extendedResp(1) LDAP_START_TLS_	OID		
4	32 3.056921	192.0.2.5	192.0.2.15	TLSv1.2	313 Client Hello			
	33 3.057324	192.0.2.15	192.0.2.5	TLSv1.2	1515 Server Hello, Certificate, Serv	/er Key	Exchange, Certificate Req	uest, Server Hello Done
	35 3.000532	192.0.2.5	192.0.2.15	TLSV1.2	173 Change Cipher Spec Encounted h	ge, Cha	hge Cipner Spec, Encrypted	Handshake Plessage
	50 5.001070	192.0.2.13	192.0.2.9	16341.2	175 change cipher spec, encrypted r	101103110	Ke Hessage	
PF	rame 33: 1515 by	tes on wire (12120 b	oits), 1515 bytes captu	red (12120	bits) on interface \Device\NPF_{3EAD5	E9F-B60	CB-4EB4-A462-217C1A10A8FE},	, id 0
P	thernet II, Src:	VMware_69:c8:c6 (00	0:00:29:69:08:06), Dst:	Whware_29:	ct:2d (00:0c:29:29:ct:2d)		44.00.00	16 M
1.5	nternet Protocol	version 4, Src: 192	2.0.2.15, Dst: 192.0.2.	5	Aska 270 Lass 1440		Cisco Firepower Manageme	int Co X +
11	cancert Laver S	acunity	ne: 565, 050 Port: 525	04, Sey: 4/	, ACK: 279, Len: 1449			Norma (and a series and a 20027422 Ed. et al. a.
1.7.7	4 TLSv1.2 Record	Laver: Handshake Pr	otocol: Multiple Hands	hake Messag	PC		← → G ■ fmc/pia	tinum/authconfig.cgl?id=72657452-51c1-11ea-
	Content Type	: Handshake (22)	otocoar noacapac nonos	and the stop				isian Davison Objects AMD Intellia
	Version: TLS	1.2 (0x0303)					Overview Analysis Pol	icles Devices Objects AMP Intellig
	Length: 1444						Config	uration Users Domains Integration
	Handshake Pr	otocol: Server Hell	0			- 1		
	₄ Handshake Pr	otocol: Certificate				_	Users User Roles	External Authentication
	Handshake	Type: Certificate	(11)			_		
	Length: 1	124				_		
	Certifica	ites Length: 1121				_	External Authentication	on Object
	₄ Certifica	tes (1121 bytes)				_	Authentication Method	
	Certif	icate Length: 1118					Authentication Piethod	LOAP
	4 Certif	icate: 3082045a3082	0342a00302010202133200	00000456c380	3c8 id-at-commonName=WIN.SEC-LAB	1d-	CAC	Use for CAC authentication and authorization
	V Sig	nedCertificate					Name *	SEC-LDAP
	v aig	ding: 0	hazsowithksAEncryption	,		_		
	Pau	cvoted: 3645eb11287	88982e7a5178f36022fa30	e77bad1043b	bbdd	_	Description	
	b Handshake Pr	otocol: Server Key	Exchange			_	Server Type	MS Active Directory V Set Defaults
	Handshake Pr	otocol: Certificate	Request			_		
	4 Handshake Pr	otocol: Server Hell	o Done				-	
	Handshake	Type: Server Hello	Done (14)				Primary Server	
	Length: 0						Hast Name/ID Address 8	WITH CEC LAD
							Host Humo IP Address	WIN SEC-LAD
							Port *	389

Información Relacionada

<u>Cuentas de usuario para acceso a la gestión</u>

- Vulnerabilidad de omisión de autenticación del protocolo ligero de acceso a directorios de <u>Cisco Firepower Management Center</u>
- <u>Configuración del objeto de autenticación LDAP en el sistema FireSIGHT</u>
- Soporte Técnico y Documentación Cisco Systems

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).