# Configurazione dell'integrazione di Active Directory con ASDM per l'autenticazione Single Sign-On e Captive Portal (gestione integrata)

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Passaggio 1. Configurare l'agente utente Firepower per Single Sign-On. Passaggio 2. Integrare Firepower Module (ASDM) con User Agent. Passaggio 3. Integrare Firepower con Active Directory. Passaggio 3.1 Creazione del realm. Passaggio 3.2 Aggiungere l'indirizzo IP/il nome host del server delle directory. Passo 3.3 Modifica della configurazione del realm. Passaggio 3.4 Scaricare il database degli utenti. Passaggio 4. Configurare il criterio di identità. Passaggio 5. Configurare i criteri di controllo di accesso. Passaggio 6. Distribuire i criteri di controllo di accesso. Passaggio 7. Monitorare gli eventi utente. Verifica Connettività tra Firepower Module e User Agent (autenticazione passiva) Connettività tra FMC e Active Directory Connettività tra l'appliance ASA e il sistema terminale (autenticazione attiva) Configurazione delle policy e distribuzione delle policy Risoluzione dei problemi

Informazioni correlate

## Introduzione

Questo documento descrive la configurazione dell'autenticazione Captive Portal (Active Authentication) e Single Sign-On (Passive Authentication) sul modulo Firepower con ASDM (Adaptive Security Device Manager).

## Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance) e di ASDM
- Knowledge Base del modulo FirePOWER
- LDAP (Light Weight Directory Service)
- Firepower UserAgent

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) con software versione 5.4.1 e successive.
- Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

L'autenticazione Captive Portal o l'autenticazione attiva richiede una pagina di accesso e le credenziali utente sono necessarie affinché un host possa accedere a Internet.

L'autenticazione Single Sign-On o passiva fornisce all'utente l'autenticazione senza interruzioni per le risorse di rete e l'accesso a Internet senza immettere più volte le credenziali utente. L'autenticazione Single Sign-On può essere eseguita tramite l'agente utente Firepower o l'autenticazione del browser NTLM.

Nota: autenticazione Captive Portal, l'appliance ASA deve essere in modalità di routing.

Nota: Il comando Captive Portal è disponibile in ASA versione 9.5(2) e successive.

## Configurazione

## Passaggio 1. Configurare l'agente utente Firepower per Single Sign-On.

Questo articolo spiega come configurare Firepower User Agent nel computer Windows:

Installazione e disinstallazione di Sourcefire User Agent

## Passaggio 2. Integrare Firepower Module (ASDM) con User Agent.

Accedere ad ASDM, selezionare **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources** (Configurazione ASA FirePOWER > Integrazione > Origini identità), quindi fare clic sull'opzione **User Agent**. Dopo aver fatto clic sull'opzione **Agente utente** e aver configurato l'indirizzo IP del sistema Agente utente. fare clic su **Add** (Aggiungi), come mostrato nell'immagine:

O O ASA FirePOWER Configurat	○ ○ ○ <u>Configuration &gt; A</u>	SA FirePOWER Config	uration > Integration > I	dentity Sources	
▶ 🗐 Policies					
🕨 👼 Device Management	Cisco CSI Realms	Identity Sources	Remote Management	eStreamer	
🕨 🧒 Object Management	Cibeo cox ricamio	ruchaty bources	Remote Hanagement	cotreamer	
▶ 🏠 Local					You have unsaved changes 🛛 🔀 Cancel 🛛 🔲 Save
ன System Information					
📑 Updates					
🖺 Licenses	Identity Sources				
🔻 🧰 Tools	Service Type	None	Identity Services Engine	Liser Agent	
🗑 Backup Restore			Identity Services Engine	User Agent	
Scheduling					New Agent
🕼 Import Export	Host Name/IP Address	Liser Agent			2 X
Jrouble shooting	-	User Agent			
🔻 🍡 Integration					
Cisco CSI		Host Name/IP Addre	ess 192.168.10.11		
🔏 Realms					
凝 Identity Sources					
🔯 Remote Management				Add Cano	cel
📝 eStreamer					

Fare clic sul pulsante Salva per salvare le modifiche.

## Passaggio 3. Integrare Firepower con Active Directory.

Passaggio 3.1 Creazione del realm.

Accedere ad ASDM, selezionare **Configuration > ASA FirePOWER Configuration > Integration > Realms** (Configurazione ASA FirePOWER > Integrazione > Realm). Fare clic su **Aggiungi nuovo realm**.

Nome e descrizione: fornire un nome o una descrizione per identificare in modo univoco il realm.

Tipo: AD

Dominio primario AD: nome di dominio di Active Directory (nome NETBIOS).

Nome utente directory: specificare < nomeutente >.

Password directory: Specificare la <password>.

Nome distinto di base: nome distinto dell'unità organizzativa di dominio o specifica d	a cui il
sistema avvierà una ricerca nel database LDAP.	

DN gruppo: Specificare il DN del gruppo.

Attributo gruppo: Specificare l'opzione Member dall'elenco a discesa.

O O ASA FirePOWER Configurat	○ ○ ○ Configu	uration > A	SA FireP	OWER Conf	iguratio	<u>1 &gt; Integration</u>	> <u>Re</u>	<u>alms</u>						
Policies														
Device Management	Cisco CSI	Realms	Identi	ity Sources	Rem	ote Manageme	nt	eStreamer						
Object Management												Compare r	ealms	New realm
LOCAI     System Information	<u> </u>				_						-			
Undates	Name		D	escription		Туре	Bas	e DN	Group DN		Group At	ttribute	State	
1 Licenses		Add Nov	, Boolm	、 、						2 V				
🔻 🔂 Tools		Aud New	Realin	1						. ^				
🕘 Backup Restore		Name *		s	ervertest									
🧱 Scheduling							_							
🕒 Import Export		Descripti	ion											
Troubleshooting		Type *		A	D		~							
<ul> <li>Integration</li> <li>Class C(I)</li> </ul>		AD Prima	ary Domai	in * s	ervertest.c	om		ex: domain.com						
		Director	/ Ilcornam		on/ortoct) a	dmin		ev: user@domain						
		Directory	, oscinari	3	er ver test (a	umm		ex. user@domain						
Remote Management		Directory	/ Password	d *	•••••									
Streamer		Base DN	*	d	c=serverte	st,dc=com		ex: ou=user,dc=cis	co,dc=com					
_		Group D	N *	c	n=TAC.ou=	Security-Team.dc	=serv	ex: ou=group,dc=c	isco,dc=com					
		Carry A				,		5						
		Group A	ttribute	ľ	lember		•							
		* Requir	ed Field											
								ОК	Cancel					

Fare clic su **OK** per salvare la configurazione.

In questo articolo vengono illustrati i valori del DN di base e del DN gruppo.

Identifica attributi oggetto LDAP di Active Directory

### Passaggio 3.2 Aggiungere l'indirizzo IP/il nome host del server delle directory.

Per specificare l'indirizzo IP/nome host del server AD, fare clic su Aggiungi directory.

Nome host/Indirizzo IP: configurare l'indirizzo IP o il nome host del server AD.

Port: Specificare il numero di porta LDAP di Active Directory (Predefinito 389).

**Crittografia/certificato SSL: (facoltativo)** Per crittografare la connessione tra FMC e server AD, fare riferimento a questo articolo:

Verifica dell'oggetto di autenticazione sul sistema FireSIGHT per l'autenticazione di Microsoft AD su SSL/T...

O O O ASA FirePOWER Configurat	000 <u>Conf</u>	iguration > ASA Fir	ePOWER Configurat	<u>ion &gt; Integra</u>	tion > <u>Realm</u>	<u>IS</u>	
<ul> <li>Folicies</li> <li>Device Management</li> <li>Object Management</li> <li>Coal</li> </ul>	Servert	est					
Updates Licenses	Directory	Realm Configuratio	n User Download		_	_	_
▼ 💼 Tools	URL (Hostna	me/IP Address and P	ort)				Encryption
iiii Scheduling		Add directory				? ×	
<ul> <li>Troubleshooting</li> <li>Integration</li> <li>Circo CSI</li> </ul>		Hostname / IP Address	192.168.10.11			_	
Realms Light Identity Sources		Port Encryption	389 STARTTLS LDA	PS 💿 None			
🧕 Remote Management 📝 eStreamer		SSL Certificate		▼ ③			
				ОК	Test	Cancel	

Clic **Test** per verificare la connessione del CCP al server AD. Fare clic su **OK** per salvare la configurazione.

Passo 3.3 Modifica della configurazione del realm.

Per modificare e verificare la configurazione dell'integrazione del server AD, passare a **Configurazione realm**.

Passaggio 3.4 Scaricare il database degli utenti.

Passare a **Download utente** per recuperare il database utenti dal server AD.

Selezionare la casella di controllo per scaricare **utenti e gruppi** e definire l'intervallo di tempo con cui il modulo Firepower contatta il server AD per scaricare il database utenti.

Selezionare il gruppo e aggiungerlo all'opzione Includi per cui si desidera configurare

l'autenticazione. Se non si sceglie di includere i gruppi, per impostazione predefinita vengono selezionati tutti i gruppi.

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration	<u> ration &gt; Integration &gt; Realms</u>	
▶      Policies			
🕨 🐻 Device Management	servertest		You have unsaved change
🕨 🧒 Object Management	Enter a description		
Local	Enter a description		
ன System Information	Y		
📑 Updates	Directory Realm Configuration User Downloa	ad	
🔛 Licenses			
🔻 🧰 Tools	Download users and groups		
3 Backup Restore	Begin automatic download at 12 👻 AM 💌 Ame	rica/New York Repeat Every 24 🕶 Hours	
Scheduling	I↓ Download Now		
🛃 Import Export			
Troubleshooting	Available Groups	Groups to Include (0)	Groups to Exclude (0)
Integration	Search by name	All available groups	None
		in create groups	
2 Identity Comment	A TAC		
Remote Menagement			
Streamer			
estreamen			
		Add to	
		Include	
		Add to	
		Exclude	
A Device Setup			
Firewall			
Remote Access VPN			
Site-to-Site VPN		Enter User Inclusion	Add Enter User Exclusion Add
ASA FirePOWER Configur			
Device <u>M</u> anagement		Store ASA FirePOWER Changes Cance	4

Fare clic su **Store ASA Firepower Changes** per salvare la configurazione dell'area di autenticazione.

Abilitare lo stato del realm e fare clic sul pulsante di download per scaricare gli utenti e i gruppi, come mostrato nell'immagine.

O O ASA FirePOWER Configurat	○ ○ O <u>Config</u>	uration > ASA F	irePOWER Config	uration	1 > Integration	> <u>Realms</u>					
Policies											
🕨 🜄 Device Management	Cisco CST	Realms Id	lentity Sources	Rem	ote Managemer	eStreamer					
🕨 🧒 Object Management	0.000 001		ientry bources		oto managemen			2.6			
► 🏠 Local								Compare re	alms 📀	New	realm
🔄 System Information	Nama		Description		Turne	Ress DN	Crown DN	Crown Attribute	Chaba		1
📑 Updates	Name		Description		туре	base DN	Group DN	Group Attribute	State		
岩 Licenses	servertest				AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tear	member		₽	🥔 📭
🔻 🧰 Tools										Down	load button
🗑 Backup Restore											
Scheduling											
🕼 Import Export							•				
Troubleshooting											
🔻 🍡 Integration											
Cisco CSI											
🔏 Realms											

## Passaggio 4. Configurare il criterio di identità.

I criteri di identità eseguono l'autenticazione dell'utente. Se l'utente non esegue l'autenticazione, l'accesso alle risorse di rete viene rifiutato. In questo modo viene applicato il controllo degli accessi basato sui ruoli (RBAC) alla rete e alle risorse dell'organizzazione.

#### Passaggio 4.1 Portale vincolato (autenticazione attiva).

Active Authentication richiede nome utente e password nel browser per identificare un'identità utente per consentire qualsiasi connessione. Il browser autentica l'utente presentando la pagina di autenticazione o esegue l'autenticazione in modo invisibile all'utente con l'autenticazione NTLM.

NTLM utilizza il browser Web per inviare e ricevere informazioni di autenticazione. L'autenticazione attiva utilizza vari tipi per verificare l'identità dell'utente. I diversi tipi di autenticazione sono:

- 1. HTTP Basic: in questo metodo, il browser richiede le credenziali dell'utente.
- 2. NTLM: NTLM utilizza le credenziali della workstation Windows e le negozia con Active Directory utilizzando un browser Web. È necessario abilitare l'autenticazione NTLM nel browser. L'autenticazione dell'utente avviene in modo trasparente senza richiedere credenziali. Offre agli utenti un'esperienza di accesso singolo.
- 3. **Negoziazione HTTP:** in questo tipo, il sistema tenta di eseguire l'autenticazione utilizzando NTLM. Se l'operazione non riesce, il sensore utilizza il tipo di autenticazione di base HTTP come metodo di fallback e richiede le credenziali dell'utente in una finestra di dialogo.
- 4. Pagina Risposta HTTP: simile al tipo di base HTTP, tuttavia, in questa pagina viene richiesto di compilare l'autenticazione in un modulo HTML personalizzabile.

Ogni browser dispone di un modo specifico per abilitare l'autenticazione NTLM e pertanto è possibile seguire le linee guida del browser per abilitare l'autenticazione NTLM.

Per condividere in modo sicuro le credenziali con il sensore instradato, è necessario installare un certificato server autofirmato o un certificato server firmato pubblicamente nei criteri di identità.

Step 3. Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt

Selezionare Configurazione > Configurazione ASA FirePOWER > Criteri > Criteri di identità. Passare alla scheda Autenticazione attiva e nell'opzione Certificato server fare clic sull'icona (+) e caricare il certificato e la chiave privata generati nel passaggio precedente utilizzando openSSL, come mostrato nell'immagine:



Fare clic su **Add rule** (Aggiungi regola) per assegnare un nome alla regola e scegliere l'azione come **Active Authentication** (Autenticazione attiva). Definire la zona di origine/destinazione, la rete di origine/destinazione per la quale si desidera abilitare l'autenticazione utente.

Passare alla scheda **Realm & Settings**. Selezionare il **Realm** dall'elenco a discesa configurato nel passaggio precedente e selezionare il **Tipo di autenticazione** dall'elenco a discesa che meglio si adatta al proprio ambiente di rete.

O O O ASA FIrePOWER Configurat	O O O Configuration > ASA F	FirePOWER Config	<u>guration &gt; Policies</u> > <u>Identi</u>	ty Policy				
🔻 🗐 Policies								_
Access Control Policy	Default Identity Po	licy					You have un	saved changes
Intrusion Policy	Add Rule							? X
💾 Files								
🔒 SSL	Name Active Authentication		Z Enabled		Insert into Catoo	<b>v</b>	Standard Bulos	<b>_</b>
🔯 Actions Alerts	Active_Addientication				into catego	лу	Standard Rules	
🚨 Identity Policy	Action Passive Authentication		<ul> <li>Realm: servertest (AD)</li> </ul>	Authentication 1	Type: HTTP Basic	xclude HTTP User-A	Agents: None	
DNS Policy		_						
🕨 🔜 Device Management	Zones Networks Ports	1					Realm & Se	ttings
🕨 🧑 Object Management								
🕨 🏠 Local	Realm * ser	rvertest (AD)		× 🖉				*
🔄 System Information	Use active authentication if p	assive authentication	n cannot identify user					
📑 Updates			·					
🔡 Licenses	Identify as Special Identities/	Guest ir authenticati	ion cannot identify user					
🔻 🧰 Tools	Authentication Type HT	TP Basic		~				
🗑 Backup Restore	Application Filters 🖒		Available Applications (83)	5		Exclude HTTP User	r-Agents (0)	
🔛 Scheduling	Search by name		Search by name			any		
🕼 Import Export						· ·		
Troubleshooting	A A Risks (Any Selected)		ABC					
🔻 🍡 Integration	Very Low	19	AdobeAIR		Add to Rule			
Cisco CSI	Low	40	Advanced Packaging Tool					
🔏 Realms	🔲 🚽 Medium	11	AirPlay					
y Identity Sources	🗐 🗾 High	6	Amazon Instant Video					
Remote Management								
🛃 eStreamer	* Description of Field							
	<ul> <li>Required Field</li> </ul>							
						ĺ	Add Ca	ancel
						(		

Passaggio 4.2 Configurazione ASA per Captive Portal.

Passaggio 1. Definire il traffico interessante che verrà reindirizzato a Sourcefire per l'ispezione.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
```

ASA(config)# policy-map global\_policy ASA(config-pmap)# class SFR\_CMAP ASA(config-pmap-c)# sfr fail-open ASA(config)#service-policy global\_policy global **Passaggio 2.** Configurare questo comando sull'appliance ASA per abilitare il portale captive.

#### ASA(config)# captive-portal interface inside port 1025

Suggerimento: captive-portal può essere abilitato a livello globale o per singola interfaccia.

**Suggerimento**: Verificare che la porta del server TCP 1025 sia configurata nell'opzione relativa alla porta della scheda Autenticazione attiva dei criteri di identità.

#### Passaggio 4.3 Single Sign-On (Autenticazione Passiva).

Nell'autenticazione passiva, quando un utente di dominio accede ad Active Directory e può autenticarlo, l'agente utente Firepower esegue il polling dei dettagli del mapping User-IP dai log di sicurezza di Active Directory e condivide queste informazioni con Firepower Module. Il modulo Firepower utilizza questi dettagli per applicare il controllo degli accessi.

Per configurare la regola di autenticazione passiva, fare clic su **Aggiungi regola** per assegnare un nome alla regola, quindi scegliere **Azione** come **Autenticazione passiva**. Definire la zona di origine/destinazione, la rete di origine/destinazione per la quale si desidera abilitare l'autenticazione utente.

Passare alla **Realm e impostazioni** . Selezionare il **Area autenticazione** dall'elenco a discesa configurato nel passaggio precedente.

Qui è possibile scegliere il metodo di fallback come **autenticazione attiva se l'autenticazione passiva non riesce a identificare l'identità dell'utente**, come mostrato nell'immagine:

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Configuration > Policies > Identity Policy	
V Policies		
Access Control Policy	Default Identity Policy	You have unsaved chang
Intrusion Policy		
💾 Files	Add Rule	? ×
🔒 SSL		
Actions Alerts	Name         Passive_Authentication         Image: Constraint of the second seco	
Identity Policy IDNS Policy	Action Passive Authentication v Realm: servertest (AD) Authentication Type: HTTP Basic Exclude HTTP User-Agents: /	
🕨 📑 Device Management	Zones Networks Ports	Realm & Settings
🕨 🧐 Object Management		
► 🏠 Local	Realm * servertest (AD)	
System Information		
📑 Updates	Use active authentication if passive authentication cannot identify user	
🔛 Licenses		
🔻 🧰 Tools		
😨 Backup Restore		
Scheduling		
🕼 Import Export		
Troubleshooting		
🔻 🍡 Integration		
Cisco CSI		
🔏 Realms		
🎍 Identity Sources		
Remote Management		
🛃 eStreamer		
	* Required Field	
	Add	i Cancel

Fare clic su Store ASA Firepower Changes per salvare la configurazione del criterio di identità.

Passaggio 5. Configurare i criteri di controllo di accesso.

Selezionare Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy (Configurazione ASA FirePOWER > Criteri > Policy di controllo dell'accesso).

Fare clic sul **criterio di identità** (angolo superiore sinistro), selezionare il criterio di identità configurato nel passaggio precedente dall'elenco a discesa e fare clic su **OK**, come mostrato nell'immagine.

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy	
Policies     Access Control Policy	ASA ASA FirePOWER	
Contraction Policy     Files     Stl     StL     Contract Alerts     Lidentity Policy     DNS Policy	Default Allow All Traffic Enter a description	
🕨 🌄 Device Management	📝 📃 Status: Access Control policy out-of-date on device	
🕨 🧑 Object Management		
► 🏠 Local	Identity Policy: None SSL Policy: None	
ன System Information 📑 Updates	Rules         Security Intelligence         HTTP Responses         Advanced	
🔛 Licenses	General Settings	ß
▼ 💼 Tools ⊗ Backup Restore	Maximum URL characters t Identity Policy ? × AN header when tracking connections	No
🧱 Scheduling 健 Import Export	Allow an Interactive Block Default Identity Policy	Ø
<ul> <li>Troubleshooting</li> <li>Integration</li> </ul>	Retry URL cache miss lookt Revert to Defaults OK Cancel iles	Disabled
Cisco CSI	Inspect traffic during policy apply Performance Settings	Ø

Fare clic su **Aggiungi regola** per aggiungere una nuova regola, passare a **Utenti** e selezionare gli utenti per i quali verrà applicata la regola di controllo di accesso, come mostrato in questa immagine e fare clic su **Aggiungi**.

O O ASA FirePOWER Configurat	OOO Configuration > ASA FirePOWER Co	nfiguration > Policies > Access Control P	<u>Policy</u>	
Policies     Access Control Policy     Intrusion Policy	ASA ASA FirePOWER			
Files	Default Allow All Traffic Enter a description		You have t	insaved changes
🚨 Identity Policy	Add Rule			? ×
<ul> <li>DNS Policy</li> <li>Device Management</li> <li>Object Management</li> </ul>	Name	Z Enabled	Insert below rule	
<ul> <li>Cost Management</li> <li>Cost Local</li> </ul>	Action 🖋 Allow	<ul> <li>IPS: no policies</li> <li>Variables: n/a Fil</li> </ul>	iles: no inspection Logging: no logging	
System Information	Zones Networks Users Application	ons Ports 🔺 URLs 🔺 ISE Attributes	Inspection Logging C	omments
	Available Realms 🖒	Available Users 🕐	Selected Users (1)	
🔻 🧰 Tools	- Search by name or value	Search by name or value	A servertest/TAC	1
School and State	Identities	servertest/*		
Scheduling	🌐 servertest	A TAC		
Troubleshooting		🚨 sunil		
🔻 🍇 Integration			Add to Rule	
Cisco CSI	1			
Julientity Sources				
Remote Management				
📝 eStreamer				
A Device Setup			Add	Cancel

Fare clic su **Archivia modifiche ASA Firepower** per salvare la configurazione dei criteri di controllo di accesso.

### Passaggio 6. Distribuire i criteri di controllo di accesso.

Ènecessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, nel modulo verrà visualizzata un'indicazione di criteri di controllo dell'accesso non aggiornata. Per distribuire

le modifiche al sensore, fare clic su **Distribuisci** e scegliere l'**opzione Distribuisci modifiche FirePOWER** quindi fare clic su **Distribuisci** nella finestra popup.

**Nota:** Nella versione 5.4.x, per applicare la policy di accesso al sensore, è necessario fare clic su Apply ASA FirePOWER Changes (Applica modifiche FirePOWER ASA)

**Nota:** Selezionare Monitoraggio > Monitoraggio di ASA Firepower > Stato task. Verificare che l'attività debba completare l'applicazione della modifica alla configurazione.

### Passaggio 7. Monitorare gli eventi utente.

Selezionare **Monitoraggio > ASA FirePOWER Monitoring > Eventi in tempo reale** per monitorare il tipo di traffico utilizzato dall'utente.

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passare a **Analisi > Utenti** per verificare l'autenticazione utente/il tipo di autenticazione/il mapping IP utente/la regola di accesso associata al flusso di traffico.

## Connettività tra Firepower Module e User Agent (autenticazione passiva)

Firepower Module utilizza la porta TCP 3306 per ricevere i dati del log delle attività dell'utente dall'agente utente.

Per verificare lo stato del servizio del modulo Firepower, usare questo comando nel FMC.

admin@firepower:~\$ netstat -tan | grep 3306 Eseguire l'acquisizione dei pacchetti nel FMC per verificare la connettività con l'agente utente.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 3306

## Connettività tra FMC e Active Directory

Il modulo Firepower utilizza la porta TCP 389 per recuperare il database utente da Active Directory.

Eseguire l'acquisizione dei pacchetti sul modulo Firepower per verificare la connettività con Active Directory.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 389

Verificare che le credenziali utente utilizzate nella configurazione del realm dispongano di privilegi sufficienti per recuperare il database utenti di Active Directory.

Verificare la configurazione del realm e assicurarsi che gli utenti/gruppi vengano scaricati e che il timeout della sessione utente sia configurato correttamente.

Passare a Monitoraggio dello stato delle attività di monitoraggio di ASA Firepower e verificare che il download dell'attività da parte di utenti/gruppi venga completato correttamente, come mostrato nell'immagine.

## Connettività tra l'appliance ASA e il sistema terminale (autenticazione attiva)

autenticazione attiva, verificare che il certificato e la porta siano configurati correttamente in Firepower module Identity policy e ASA (comando captive-portal). Per impostazione predefinita, ASA e il modulo Firepower sono in ascolto sulla porta TCP 885 per l'autenticazione attiva.

Per verificare le regole attive e il numero di accessi, eseguire questo comando sull'appliance ASA.

## ASA# show asp table classify domain captive-portal Input Table in id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false hits=10, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=6 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0 input\_ifc=inside, output\_ifc=identity Output Table: L2 - Output Table: L2 - Input Table: L2 - Input Table:

Last clearing of hits counters: Never

### Configurazione delle policy e distribuzione delle policy

Verificare che i campi Realm, Tipo di autenticazione, Agente utente e Azione siano configurati correttamente in Criteri di identità.

Verificare che i criteri di identità siano associati correttamente ai criteri di controllo di accesso.

Passare a Monitoraggio > Monitoraggio di ASA Firepower > Stato attività e verificare che la distribuzione delle policy venga completata correttamente.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Informazioni correlate

- Documentazione e supporto tecnico Cisco Systems
- Configurazione dell'integrazione di Active Directory con Firepower Appliance per l'autenticazione Single Sign-On e Captive Portal