# シングル サインオンとキャプティブ ポータル認 証(On-Box Management)用に ASDM と Active Directory を設定する

### 内容

概要 前提条件 要件 使用するコンポーネント 背景説明 設定 手順1:シングルサインオン用に Firepower ユーザ エージェントを設定する。 手順2: Firepower モジュール(ASDM)をユーザ エージェントと統合する。 手順3: Firepower を Active Directory と統合する。 手順 3.1: レルムを作成する。 手順 3.2: ディレクトリ サーバの IP アドレスとホスト名を追加する。 <u>手順 3.3:レルムの設定を変更する。</u> 手順 3.4: ユーザ データベースをダウンロードする。 ステップ4:アイデンティティポリシーを設定する。 ステップ 5: アクセス コントロール ポリシーを設定する。 手順 6: アクセス コントロール ポリシーを展開する。 手順7: 確認 Firepower モジュールとユーザ エージェント間の接続(パッシブ認証) FMC と Active Directory 間の接続 ASA とエンド システム間の接続(アクティブ認証) ポリシーの設定とポリシーの展開 トラブルシュート 関連情報

## 概要

このドキュメントでは、ASDM(Adaptive Security Device Manager)を使用して Firepower モジ ュールにキャプティブ ポータル認証(アクティブ認証)とシングルサインオン(パッシブ認証 )を設定する方法を説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ASA (適応型セキュリティ アプライアンス)ファイアウォールと ASDM の知識
- FirePOWER モジュールの知識
- Light Weight Directory Service (LDAP)
- Firepower ユーザ エージェント

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 5.4.1 以降を実行する ASA FirePOWER モジュール(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。
- ソフトウェア バージョン 6.0.0 以降を実行する ASA FirePOWER モジュール(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

### 背景説明

キャプティブ ポータル認証またはアクティブ認証では、ログイン ページが表示され、ホストがイ ンターネットにアクセスするためにユーザ クレデンシャルが必要になります。

シングルサインオンまたはパッシブ認証では、ユーザ クレデンシャルを複数回入力する必要のな い、ネットワーク リソースやインターネット アクセスのためのシームレスな認証をユーザに提供 します。シングルサインオン認証は、Firepower ユーザ エージェントまたは NTLM ブラウザ認証 のいずれかによって実現できます。

注:キャプティブポータル認証、ASAはルーテッドモードである必要があります。

注: キャプティブ ポータル コマンドは、ASA バージョン 9.5(2) 以降で使用できます。

### 設定

#### 手順1:シングルサインオン用に Firepower ユーザ エージェントを設定する。

次の記事では、Windows マシンで Firepower ユーザ エージェントを設定する方法について説明 します。

Sourcefire ユーザ エージェントのインストールとアンインストール

### ステップ2: Firepowerモジュール(ASDM)をユーザエージェントと統合します。

ASDM にログインし、[Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Identity Sources] に移動して、[User Agent] オプションをクリックします。[User Agent] オプションをク リックした後、ユーザ エージェント システムの IP アドレスを設定します。次の図のように、 [Add] をクリックします。

O O ASA FirePOWER Configurat	© © © Configuration > ASA FirePOWER Configuration > Integration > Identity Sources					
▶ 🗐 Policies						
🕨 🔜 Device Management	Cisco CSI Realms	Identity Sources	Remote Management	eStreamer		
🕨 🧒 Object Management		ruentty bources	Remote Hundgement	cotreamer		
Local					You have unsaved changes Cancel	
ன System Information						
📑 Updates						
🔡 Licenses	Identity Sources					
🔻 🧰 Tools	Service Type	None	Identity Services Engine			
🗑 Backup Restore			Additional of the second secon			
Scheduling					New Agent	
🕼 Import Export	Host Name/IP Address	User Agent			? X	
P Troubleshooting		ober Agent				
🔻 🍡 Integration						
Cisco CSI		Host Name/IP Addr	ess 192.168.10.11			
la Realms						
🏖 Identity Sources			_			
🔯 Remote Management				Add Cano	el	
📝 eStreamer						

[Save] ボタンをクリックして、変更を保存します。

### 手順3: Firepower を Active Directory と統合する。

手順 3.1: レルムを作成する。

ASDM にログインし、[Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] **に移動します。**[Add a New Realm] をクリックします。

名前と説明:レルムを一意に識別するための名前と説明を指定します。

タイプ: AD

ADプライマリドメイン: Active Directoryのドメイン名(NETBIOS名)。

Directory Username: <username>を指定します。

[Directory Password]: <パスワード> を指定します。

ベースDN:システムがLDAPデータベース内で検索を開始するドメインまたは特定のOU DN。

[Group DN]: グループの DN を指定します。

[Group Attribute]:ドロップダウン リストからオプションの [Member] を指定します。

○ ○ O ASA FirePOWER Configurat	6	0 0 0 <u>Config</u>	uration > A	SA Fir	rePOWER Co	onfiguratio	n > Integration	> <u>Re</u>	alms					
Policies														
🕨 📕 Device Management		Cisco CST	Realms	Ide	antity Source	es Rem	ote Managemer	.+	eStreamer					
🕨 🧑 Object Management		CISCO COI	Realins	Iuc	antity bound		ote Hundgemen		cotreamer		_	2.5 -		
Local												Compare	e realms 🛛 😳 f	lew realm
System Information		Name			Descriptio	n	Type	Bas	e DN	Group DN		Group Attribute	State	
🛒 Updates			_		Description		1700	Dus		Group Div		Group Attribute		
Licenses			Add New	v Rea	alm						? ×			
🔻 🧰 Tools														
Backup Restore			Name *			servertest								
Scheduling								_						
🕼 Import Export			Descripti	ion										
Troubleshooting			Type *			AD		~						
🔻 🍡 Integration			AD Prim	arv Do	main *	convertest c	07		ex: domain.com					
Cisco CSI			AD THIN	ury 00	in an a	server test.c	UIII		ex. domain.com					
🌡 Realms			Directory	y Useri	name *	servertest\a	ıdmin		ex: user@domain					
ldentity Sources			Directory	v Passi	word *									
Remote Management														
📝 eStreamer			Base DN	*		dc=serverte	st,dc=com		ex: ou=user,dc=cis	co,dc=com				
			Group D	N *		cn=TAC,ou=	=Security-Team,dc=	-serv	ex: ou=group,dc=c	isco,dc=com				
			Group At	ttribut	e	Member		~						
			* Requir	ed Fie	Id									
									ОК	Cance	:I			

[OK] をクリックして、構成を保存します。

次の記事は、ベース DN およびグループ DN の値を決めるのに役立ちます。

<u>Active Directory LDAP オブジェクトの属性の特定</u>

手順 3.2: ディレクトリ サーバの IP アドレスとホスト名を追加する。

AD サーバの IP またはホスト名を指定するには、[Add directory] をクリックします。

ホスト名/IPアドレス: ADサーバのIPアドレス/ホスト名を設定します。

[Port]: Active Directory の LDAP ポート番号 (デフォルトは 389) を指定します。

暗号化/SSL証明書:(オプション)FMCとADサーバ間の接続を暗号化するには、次の記事を参照 してください。

#### <u>「SSL/TLS 経由で Microsoft AD 認証を行うための FireSIGHT システム上の認証オブジェクトの</u> <u>検証」</u>

○ ○ ○ ASA FirePOWER Configurat	- 0 0 0 <u>Confi</u>	guration > ASA Fir	ePOWER Configuration > Integ	ration > <u>Realms</u>	
► 🗐 Policies					
🕨 📕 Device Management	serverte	est			
🕨 🧑 Object Management	Enter a descrip	ation			
► 🏠 Local	Enter a descrip	Stion			
ன System Information	r				
📑 Updates	Directory	Realm Configuration	n User Download		
🔡 Licenses					
🔻 💼 Tools					
🗑 Backup Restore	URL (Hostnan	me/IP Address and P	ort)		Encryption
Scheduling		Add directory		2 ×	
🕼 Import Export		Add directory			
Troubleshooting		Hostname / IP	192 168 10 11		
🔻 🍡 Integration		Address	152.100.10.11		
Cisco CSI		Port	389		
a Realms		Enomention			
🚽 Identity Sources		Encryption	STARTILS LDAPS None		
🛽 Remote Management		SSL Certificate	▼ ○		
📝 eStreamer					
			ОК	Test Cancel	

クリック **テスト** ADサーバとのFMCの接続を確認します。[OK] をクリックして、構成を保存しま す。

#### 手順3.3:レルムの設定を変更する。

AD サーバの統合構成を変更して確認するには、[Realm Configuration] に移動します。

手順 3.4: ユーザ データベースをダウンロードする。

AD サーバからユーザ データベースを取得するために、[User Download] に移動します。

[Download users and groups] チェックボックスをオンにしてダウンロードを有効にし、ユーザ デ ータベースをダウンロードするために Firepower モジュールが AD サーバに接続する頻度を時間 間隔で定義します。

認証を設定するグループを選択し、[include] **オプションに追加します。**含めるグループを選択し ないと、デフォルトですべてのグループが選択されます。

○ ○ ○ ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration	uration > Integration > Realms		
▶ 🗐 Policies				
🕨 🐻 Device Management	servertest		You have	unsaved changes
🕨 🧒 Object Management	Enter a description			
► 🏠 Local				
ன System Information	Y			
🛒 Updates	Directory Realm Configuration User Downlo	ad		
Licenses				
🔻 🧰 Tools	Download users and groups			
🗑 Backup Restore	Begin automatic download at 12 V AM V Ame	erica/New York Repeat Every 24 🗸 Hours		
Scheduling	La Download Now			
🕼 Import Export				
Troubleshooting	Available Groups	Groups to Include (0)	Groups to Exclude (0)	
V 🔌 Integration	Search by name	All available groups	None	
Cisco CSI		All available groups	None	
Realms	🝰 TAC			
Jentity Sources				
Remote Management				
eStreamer				
		Add to		
		Include		
		Add to		
		Exclude		
💑 <u>D</u> evice 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	Cancel	

[Store ASA Firepower Changes] をクリックして、レルムの構成を保存します。

レルムの状態を有効にし、ダウンロード ボタンをクリックしてユーザとグループをダウンロード します(次の図を参照)。

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA Find	rePOWER Configuration	1 > Integration	> <u>Realms</u>				
Policies								
🕨 🔜 Device Management	Cisco CSI Realms Ide	entity Sources Rem	ote Managemer	eStreamer				
🕨 🧒 Object Management			ote Hanagemen			2.6		
🕨 🏠 Local						Compar	e realms 🛛 😳	New realm
🔄 System Information	Nama	Description	Turne	Base DN	Crown DN	Crown Attribute	Chata	
📑 Updates	Name	Description	туре	base DN	Group DN	Group Attribute	State	
🔡 Licenses	servertest		AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tear	n member	$\checkmark$	🕁 🥔 🗓
🔻 💼 Tools								Download button
🗑 Backup Restore								
Scheduling								
🕼 Import Export					•			
Troubleshooting								
🔻 🍡 Integration								
Cisco CSI								
🔏 Realms								

### ステップ4:アイデンティティポリシーを設定する。

アイデンティティ ポリシーはユーザ認証を実行します。ユーザが認証されないと、ネットワーク リソースへのアクセスが拒否されます。ポリシーを設定すると、ロールベース アクセス コントロ ール(RBAC)が組織のネットワークとリソースに適用されます。

手順 4.1: キャプティブ ポータル (アクティブ認証)。

アクティブ認証は、ブラウザでユーザ名とパスワードの入力を要求し、ユーザのアイデンティティを特定して、接続を許可します。ブラウザは、認証ページを表示することで、または NTLM 認証を使用してサイレントに、ユーザを認証します。 NTLM は、Web ブラウザを使用して、認証情報を送受信します。アクティブ認証は、さまざまな方式を使用してユーザのアイデンティティを確認します。認証の方式は次のとおりです。

1. HTTP Basic:この方法では、ブラウザがユーザーの資格情報を要求します。

- NTLM: NTLM は、Windows ワークステーション クレデンシャルを使用し、Webブラウザ を使用してそれを Active Directory とネゴシエートします。ブラウザで NTLM 認証を有効に する必要があります。ユーザ認証は、クレデンシャルを要求することなく透過的に行われま す。ユーザにシングルサインオン環境を提供します。
- HTTP Negotiate:このタイプでは、システムはNTLMを使用して認証を試みます。失敗した場合、センサーはフォールバック方式としてHTTP Basic認証タイプを使用し、ユーザクレデンシャルのダイアログボックスを表示します。
- 4. HTTP応答ページ:これはHTTP基本タイプに似ていますが、ここでユーザはカスタマイズ可能なHTML形式で認証を入力するように求められます。

各ブラウザには NTLM 認証を有効にする固有の方法があり、そのため、NTLM 認証を有効にする にはブラウザのガイドラインに従います。

ルーテッド センサーとクレデンシャルを安全に共有するには、自己署名サーバ証明書または公開 署名サーバ証明書をアイデンティティ ポリシーにインストールする必要があります。

Generate a simple self-signed certificate using openSSL -

```
Step 1. Generate the Private key
openssl genrsa -des3 -out server.key 2048
```

Step 3. Generate the self-signed Certificate.

openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt

[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy]に移動します.次に 、[Active Authentication]タブに移動し、[Server Certificate]オプションで、アイコン(+)をクリック します 図に示すように、openSSLを使用して前の手順で生成した証明書と秘密キーをアップロー ドします。

O O ASA FirePOWER Configurat	O O Configuration > ASA Fire	POWER Configuration >	Pol	icies > Identity Policy	
▼					
🚦 Access Control Policy	Default Identity Polic	٧			You have unsaved changes
Intrusion Policy	Identify Policy	· <b>/</b>			
🖺 Files	Identity Policy				
🔒 SSL					
🔯 Actions Alerts				Add Known Internal Certificate	? X
& Identity Policy					
DNS Policy				Name: Server_Cert	
🕨 🔜 Device Management	Rules Active Authentication			Certificate Data or, choose a file: Browse	
🕨 🧒 Object Management			-		
🕨 🏠 Local	Server Certificate * None	v	0	BEGIN CERTIFICATE MIIDkDCCAvmaAwIBAaIJAPTn5TIH1vBdMA0GCSaGSIb3D0FBB0LJAMIGNM0swC0YF	)
ன System Information	Dank *			VQQGEwJJTjELMAkGA1UECBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UE	
📑 Updates	1025		(88	ChMFQ0ITQ08xDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5j	
🔡 Licenses	Maximum login attempts * 3		(0	ODE1MzE0NVoXDTI2MDUxNjE1MzE0NVowqY0xCzAJBqNVBAYTAklOMQswCQYDVQQ	I I
🔻 🧰 Tools				EwJLQTESMBAGA1UEBxMJQkFOR0FMT1JFMQ4wDAYDVQQKEwVDSVNDTzEMMAoGA	1UE
3 Backup Restore	Active Authentication Response Pa	age		CXMDVEFDMR0wGAYDVQQDEXFDQS5ZZXJ2ZXJ0ZXN0LmNvD1EJMCEGCSqGS1D3DQE ARYLIYWRtaW5Ac2VvdmVvdGVzdC5ib20waZ8wDOY1KaZ1hvcNAOEBBQADaY0AMIG1	J
Scheduling	Authentication Type.	iggers an identity rule with HT	IIPF		
💽 Import Export				Key or, choose a file: Browse	
Troubleshooting	System-provided	¥	- Co	BEGIN RSA PRIVATE KEY	
Integration				Proc-Type: 4,ENCRYPTED	
Cisco CSI	* Required when using Active Authent	ication		DER-INTO: DES-EDE3-CBC,B3542C/C6/0DC91/	
A Realms				mLeuBJX5T2apbAnOLR+sLYAPqJKxiXigDjR/1RM3WDPK3WHnCvn7Rdwkvw3xbdBC	
a name to Management				G6u2y+J9wNIIC6sfg4ItjX2Imbkp6LaX0fhlJunUbktSjAKvmi7cIno0JipkfQi3	
				LDFOB421fgxqALiVNKcfuXXzY7x6cbpc0ZjB8duJgKIRABwcaSKyP+4ZE/I77NVj	
estreamer				tbYSoMw8uKR8BljLTJ1/+YpWFT2bBx4g6iQn9UO4RosakCBKdQLIJwIi49GpOIP2	
				Encrypted and the password is:	
S Device Setur				Store ASA FirePOWER	Changes Cancel
ACDM IDM					
Remote Access VPN					
Site-to-Site VPN					
ASA FirePOWER Configur				Store ASA FirePOWER Changes Cancel	

[Add rule] をクリックしてルールの名前を指定し、アクションとして [Active Authentication] を選択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信元/宛先ネットワークを定義します。

[Realm & Settings] **タブに移動します。**[Realm] **ドロップダウン リストから前の手順で設定したレ ルムを選択し、[Authentication Type]** ドロップダウン リストからネットワーク環境に最適な認証 方式を選択します。

O O ASA FIREPOWER Configurat	O O O Configuration > AS	A FirePOWER Confi	<u>guration &gt; Policies</u> > <u>Ident</u>	ity Policy				
▼ 🗐 Policies								
Sccess Control Policy	Default Identity	Policy					You have	unsaved changes
Intrusion Policy	Add Rule							? ×
💾 Files								
🔒 SSL	Name Active Authentication	nl	C Enabled		Insert into Catego	vrv 💌	Standard Rules	~
🔯 Actions Alerts		-			into datego	51 9	Blandard Haleb	
Identity Policy	Action Passive Authentication	on	<ul> <li>Realm: servertest (AD)</li> </ul>	Authentication	Type: HTTP Basic E	Exclude HTTP User-	Agents: None	
DNS Policy								
🕨 📕 Device Management	Zones Networks Pe	orts					Realm &	Settings
🕨 🤜 Object Management								
► 🏠 Local	Realm *	servertest (AD)		▼ Ø				*
System Information	Use active authentication	if passive authenticatio	n cannot identify user					
📑 Updates	Identify as Special Identi	tion/Cuast if authoriticat	ion connot identify upor					
🔛 Licenses		ties/Guest in authenticat	ion cannot identify user					
🔻 🧰 Tools	Authentication Type	HTTP Basic		*				
🤡 Backup Restore	Application Filters 🖒		Available Applications (83)	5		Exclude HTTP Use	r-Agents (0)	
🧱 Scheduling	Search by name		Search by name			anv		
🕼 Import Export								
🖉 Troubleshooting	A 🗾 Risks (Any Selected)		ABC	(C				
🔻 🔌 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					<i>y</i>			
🛃 eStreamer	The second Field							
	* Required Field							
							Add	Cancel

手順 4.2:キャプティブ ポータルの ASA 構成。

手順1: 検査のために Sourcefire にリダイレクトするインタレスティング トラフィックを定義します。

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-cmap)# match access-list SFR\_ACL

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 手順2:キャプティブ ポータルを有効にするために ASA で次のコマンドを設定します。

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

captive-portal

[Active Authentication] TCP 1025

手順 4.3: シングルサインオン(パッシブ認証)。

パッシブ認証では、ドメイン ユーザがログインして、AD の認証を行うことができる場合、 Firepower ユーザ エージェントは AD のセキュリティ ログから ユーザと IP マッピングの詳細を ポーリングし、この情報を Firepower モジュールと共有します。Firepower モジュールはこれらの詳細を使用して、アクセス制御を適用します。

パッシブ認証ルールを設定するには、[Add rule] をクリックしてルールの名前を指定し、[Action] として [Passive Authentication] を選択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信 元/宛先ネットワークを定義します。

次の場所に移動します。レルムと設定 tab.選択 領域 ドロップダウンリストから選択します。

フォールバック方法として、[Active authentication if passive authentication cannot identify the user identity] を選択できます(次の図を参照)。

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Configuration > Policies > Identity Policy	
Policies		
Access Control Policy	Default Identity Policy	You have unsaved change
Intrusion Policy		
💾 Files	Add Rule	? X
🔒 SSL		
X Actions Alerts	Name Passive_Authentication	
DNS Policy	Action Passive Authentication   Realm: servertest (AD) Authentication Type: HTTP Basic Exclude HTTP User-Agents:	
🕨 📕 Device Management	Zones Networks Ports	Realm & Settings
🕨 🧒 Object Management		) ····································
► 🏠 Local	Realm * servertest (AD)	
ன System Information		
📑 Updates	Use active authentication if passive authentication cannot identify user	
🔛 Licenses		
🔻 🧰 Tools		
lackup Restore		
Scheduling		
🕼 Import Export		
Proubleshooting		
🔻 🍡 Integration		
Cisco CSI		
🔏 Realms		
凝 Identity Sources		
🔯 Remote Management		
📴 eStreamer		
	* Required Field	
	Ad	ld Cancel

[Store ASA Firepower Changes] をクリックして、アイデンティティ ポリシーの設定を保存します。

## ステップ 5 : アクセス コントロール ポリシーを設定する。

[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] に移動します。

[Identity Policy] (左上隅)をクリックして、ドロップダウン リストから前の手順で設定したアイ デンティティポリシーを選択し、[OK] をクリックします(次の図を参照)。

○ ○ ○ ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy	
Policies     Access Control Policy	ASA FirePOWER	
<ul> <li>         Intrusion Policy     </li> <li>         Files     </li> <li>         SSL     </li> <li>         Actions Alerts     </li> <li>         Identity Policy     </li> <li>         DNS Policy     </li> </ul>	Default Allow All Traffic Enter a description	
Device Management	📝 📑 Status: Access Control policy out-of-date on device	
🕨 🧑 Object Management		
Accal     System Information     Indates	Identity Policy: None     SSL Policy: None       Rules     Security Intelligence     HTTP Responses       Advanced	
Licenses	General Settings // Transport/Network Layer Preprocessor Settings	Ø
Tools Backup Restore	Maximum URL characters t Identity Policy ? × AN header when tracking connections	No
Scheduling	Allow an Interactive Block Default Identity Policy	Ø
Troubleshooting	Retry URL cache miss look Revert to Defaults OK Cancel iles	Disabled
Cisco CSI	Inspect traffic during policy apply Performance Settings	Ø

クリック **ルールの追加** 新しいルールを追加するには、 **[ユーザ(Users)]** 次の図に示すように、 アクセスコントロールルールを適用するユーザを選択し、[Add]をクリックします.

○ ○ O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Con	nfiguration > Policies > Access Control Pol	licy	
Policies     Access Control Policy     Ontrucion Policy	ASA ASA FirePOWER			
Files	Default Allow All Traffic			You have unsaved changes
🛅 SSL	Enter a description			
Actions Alerts	Add Bule			? X
Device Management	Name	Enabled	Insert below rule 💙 1	
🕨 🧒 Object Management	Action Allow	TDS: no nolicies Variables: n/a File	e: no inspection logging: no logging	
🕨 🏠 Local	Action	v rest no policies variables. Il a file	a no mapeerion cogging. No logging	
System Information	Zones Networks Users Application	ons Ports 🔺 URLs 🔺 ISE Attributes	Inspection	Logging Comments
📑 Updates	Available Realms	Available Licers	Selected Users (1)	
Licenses			Selected Users (1)	
🔻 🔂 Tools	Search by name or value	Search by name or value	A servertest/TAC	1
Backup Restore	f Special Identities	servertest/*		
limport Export	() servertest	A TAC		
		sunil		
V 🔌 Integration			Add to Bule	
Cisco CSI			Add to hard	
🔏 Realms				
🍛 Identity Sources				
Remote Management	1			
🛃 eStreamer				
A Device Setup				Add Cancel

#### クリック ASA Firepowerの変更の保存 アクセスコントロールポリシーの設定を保存します。

### 手順6:アクセスコントロールポリシーを展開する。

アクセス コントロール ポリシーを展開する必要があります。ポリシーを適用する前に、モジュー ルにアクセスコントロールポリシーの最新の情報が表示されます。センサーに変更を展開するに は、[Deploy]をクリックし、[Deploy FirePOWER Changes]オプションを選択して、ポップアップ ウィンドウの[Deploy]をクリックします。

**注:**バージョン 5.4.x では、アクセス ポリシーをセンサーに適用するには、[Apply ASA FirePOWER Changes] をクリックする必要があります。

**注**: [Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。構成の変更を 適用するには、タスクを完了する必要があります。

#### 手順7:

[Monitoring] > [ASA FirePOWER Monitoring] > [Real-Time Eventing] に移動し、ユーザが使用して いるトラフィックの種類を監視します。

### 確認

ここでは、設定が正常に機能しているかどうかを確認します。

[Analysis] > [Users] に移動し、トラフィック フローに関連付けられているユーザ認証、認証の種 類、ユーザ IP マッピング、アクセス ルールを確認します。

### Firepower モジュールとユーザ エージェント間の接続(パッシブ認証)

ユーザ エージェントからユーザ アクティビティ ログ データを受信するために、Firepower モジ ュールは TCP ポート 3306 を使用します。

Firepower モジュールのサービス ステータスを確認するには、FMC で次のコマンドを使用します。

admin@firepower:~\$ netstat -tan | grep 3306 ユーザ エージェントとの接続を確認するには、FMC でパケット キャプチャを実行します。

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

#### FMC と Active Directory 間の接続

Active directory からユーザ データベースを取得するために、Firepower モジュールは TCP ポート 389 を使用します。

Active Directory との接続を確認するには、Firepower モジュールでパケット キャプチャを実行します。

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

レルムの設定で使用されているユーザ クレデンシャルに、AD のユーザ データベースを取得する のに十分な権限があることを確認します。

レルムの設定を調べて、ユーザまたはグループがダウンロードされること、およびユーザ セッションのタイムアウトが正しく設定されていることを確認します。

[Monitoring ASA Firepower Monitoring Task Status] に移動し、タスク ユーザとグループのダウン ロードが正常に完了したことを確認します(次の図を参照)。

#### ASA とエンド システム間の接続(アクティブ認証)

アクティブ認証の場合、Firepower モジュールのアイデンティティ ポリシーおよび ASA で証明書 とポートが正しく設定されていることを確認します(キャプティブ ポータル コマンド)。 デフ ォルトでは、ASA と Firepower モジュールは、TCP ポート 885 でアクティブ認証をリッスンし ます。

アクティブなルールとそのヒット数を調べるには、ASA で次のコマンドを実行します。

#### 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, port=1025, tag=any, dscp=0x0
 input\_ifc=inside, output\_ifc=identity

Output Table:

L2 - Output Table:

Last clearing of hits counters: Never

#### ポリシーの設定とポリシーの展開

[Identity Policy] で [Realm]、[Authentication type]、[User agent]、[Action] の各フィールドが正し く設定されていることを確認します。

アイデンティティ ポリシーがアクセス コントロール ポリシーと正しく関連付けられていることを確認します。

[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動し、ポリシーの展開が正常に完 了していることを確認します。

# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

### 関連情報

- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>
- シングルサインオンとキャプティブポータルの認証用に FirePOWER アプライアンスを含む Active Directory の統合を設定する