Configurer l'intégration Active Directory avec ASDM pour l'authentification unique et l'authentification captive du portail (gestion intégrée)

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration Étape 1. Configurez l'agent utilisateur Firepower pour l'authentification unique. Étape 2. Intégrez le module Firepower (ASDM) à l'agent utilisateur. Étape 3. Intégrez Firepower à Active Directory. Étape 3.1 - Créez le domaine. Étape 3.2 - Ajoutez l'adresse IP/le nom d'hôte du serveur d'annuaire. Étape 3.3 - Modifiez la configuration du domaine. Étape 3.4 - Téléchargez la base de données des utilisateurs. Étape 4. Configurez la stratégie d'identité. Étape 5. Configurez la stratégie de contrôle d'accès. Étape 6. Déployez la stratégie de contrôle d'accès. Étape 7. Surveiller les événements utilisateur. Vérification Connectivité entre le module Firepower et l'agent utilisateur (authentification passive) Connectivité entre FMC et Active Directory Connectivité entre ASA et système d'extrémité (authentification active) Configuration des politiques et déploiement des politiques Dépannage Informations connexes

Introduction

Ce document décrit la configuration de l'authentification du portail captif (authentification active) et de l'authentification unique (authentification passive) sur le module Firepower à l'aide d'ASDM (Adaptive Security Device Manager).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du pare-feu ASA (Adaptive Security Appliance) et de l'ASDM
- Connaissances du module FirePOWER
- Service LDAP (Light Weight Directory Service)
- Agent utilisateur Firepower

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Modules ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) exécutant le logiciel version 5.4.1 et ultérieure.
- Module ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) exécutant le logiciel version 6.0.0 et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Captive Portal Authentication ou Active Authentication demande une page de connexion et les informations d'identification de l'utilisateur sont requises pour qu'un hôte puisse accéder à Internet.

L'authentification à connexion unique ou passive permet à un utilisateur d'obtenir une authentification transparente pour les ressources réseau et l'accès à Internet sans saisir plusieurs fois les informations d'identification de l'utilisateur. L'authentification à connexion unique peut être obtenue soit par l'agent utilisateur Firepower, soit par l'authentification du navigateur NTLM.

Remarque : l'authentification du portail captif, ASA doit être en mode routé.

Note: La commande Captive Portal est disponible dans ASA version 9.5(2) et versions ultérieures.

Configuration

Étape 1. Configurez l'agent utilisateur Firepower pour l'authentification unique.

Cet article explique comment configurer Firepower User Agent dans l'ordinateur Windows :

Installation et désinstallation de Sourcefire User Agent

Étape 2. Intégrez le module Firepower (ASDM) à l'agent utilisateur.

Connectez-vous à ASDM, accédez à Configuration > ASA FirePOWER Configuration > Integration > Identity Sources et cliquez sur l'option User Agent. Après avoir cliqué sur l'option Agent

utilisateur et configuré l'adresse IP du système Agent utilisateur. cliquez sur **Ajouter**, comme l'illustre l'image :

O O ASA FirePOWER Configurat	0 0 0 Configuration > ASA FirePOWER Configuration > Integration > Identity Sources
Policies	
🕨 👼 Device Management	Cisco CST Realms Identity Sources Remote Management eStreamer
🕨 🧒 Object Management	
▶ 🏠 Local	You have unsaved changes 🔗 Cancel 🛛 🔲 Save
ன System Information	
📑 Updates	
🔡 Licenses	Identity Sources
🔻 💼 Tools	Service Type None Education Engine Likes Apart
🗑 Backup Restore	
Scheduling	New Agent
🕼 Import Export	Host Name/IP Address Licer Agent 2 x
July Troubleshooting	User Agent
🔻 🍡 Integration	
Cisco CSI	Host Name/IP Address 192.168.10.11
🔏 Realms	
🏖 Identity Sources	
🔯 Remote Management	Add Cancel
📝 eStreamer	

Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Étape 3. Intégrer Firepower à Active Directory.

Étape 3.1 - Créez le domaine.

Connectez-vous à ASDM, accédez à **Configuration > ASA FirePOWER Configuration > Integration > Realms.** Cliquez sur **Ajouter un nouveau domaine**.

Nom et description : Donnez un nom/une description pour identifier le domaine de manière unique.

Type : AD

Domaine principal AD : Nom de domaine d'Active Directory (nom NETBIOS).

Nom d'utilisateur du répertoire : spécifiez le < nom d'utilisateur>.

Mot de passe du répertoire : Spécifiez le < mot de passe>.

Nom unique de base : Domaine ou Nom unique d'unité d'organisation spécifique à partir duquel le système lancera une recherche dans la base de données LDAP.

DN du groupe : Spécifiez le DN du groupe.

Attribut de groupe : Spécifiez l'option Member dans la liste déroulante.

○ ○ ○ ASA FirePOWER Configurat		O Configu	ration > AS	SA Fire	POWER Co	nfiguration	n > Integration	> <u>Re</u>	<u>alms</u>					
Policies														
🕨 📑 Device Management	Ci	isco CST	Realms	Iden	ntity Source	s Rem	ote Managemer	t I	eStreamer					
🕨 🧒 Object Management			literation	Include	int, oouree		oto managemen				_	2.6 -		
▶ 🏠 Local												Compare re	alms 😳	New realm
System Information	Na	me			Description		Type	Bas	e DN	Group DN	6	roup Attribute	State	
📑 Updates					Description		1990	Dust		Group Div		noup Attribute	Juic	
Licenses			Add New	/ Real	m					? >	<			
🔻 🧰 Tools														
Backup Restore			Name *			servertest								
Scheduling			Descripti	ion				_						
E Import Export			Descripti											
Troubleshooting			Type *			AD		~						
 Integration Cisco CSI 			AD Prima	ary Dom	nain *	servertest.c	om		ex: domain.com					
Sealms			Directory	/ Userna	ame *	servertest\a	admin		ex: user@domain					
🥁 Identity Sources			Directory	/ Passw	ord *	•••••								
Streamer			Base DN	*		dc=serverte	est,dc=com		ex: ou=user,dc=cis	co,dc=com				
			Group D	N *		cn=TAC,ou=	=Security-Team,dc	ser∿	ex: ou=group,dc=ci	sco,dc=com				
			Group At	ttribute		Member		~						
			* Requir	ed Field	I									
									ОК	Cancel				

Cliquez sur **OK** pour enregistrer la configuration.

Cet article peut vous aider à déterminer les valeurs DN de base et DN de groupe.

Identifier les attributs d'objet LDAP Active Directory

Étape 3.2 - Ajoutez l'adresse IP/le nom d'hôte du serveur d'annuaire.

Pour spécifier l'adresse IP/le nom d'hôte du serveur AD, cliquez sur Ajouter un répertoire.

Nom d'hôte/Adresse IP : configurez l'adresse IP/nom d'hôte du serveur AD.

Port : spécifiez le numéro de port LDAP Active Directory (389 par défaut).

Certificat de chiffrement/SSL : (facultatif) Pour chiffrer la connexion entre le serveur FMC et AD, reportez-vous à cet article :

<u>Vérification de l'objet d'authentification sur FireSIGHT System pour l'authentification AD Microsoft</u> <u>sur SSL/T...</u>

• • • • ASA FirePOWFR Configurat		auration > ASA FirePOWER Configuration > Integration > Pealms						
Policies		guration > AsA FilePower configuration > integration > realins						
🕨 📕 Device Management	serverte	est						
🕨 🧑 Object Management								
🕨 🏠 Local	Enter a description							
🔄 System Information								
📑 Updates	Directory	Realm Configuration User Download						
🔛 Licenses								
🔻 🧰 Tools								
🗑 Backup Restore	URL (Hostna	ne/IP Address and Port)	Encryption					
iiii Scheduling								
健 Import Export		Add directory						
dia Troubleshooting		Hostname / IP 102 168 10 11						
🔻 🍡 Integration		Address						
Cisco CSI		Port 389						
🔏 Realms								
🌡 Identity Sources		Encryption OSTARTTLS LDAPS ONON						
國 Remote Management		SSL Certificate 🗸 💿						
🔯 eStreamer								
		OK Test Cancel						

Cliquez sur **Tester** afin de vérifier la connexion de FMC avec le serveur AD. Cliquez maintenant sur **OK** pour enregistrer la configuration.

Étape 3.3 - Modifiez la configuration du domaine.

Afin de modifier et de vérifier la configuration d'intégration du serveur AD, accédez à **Configuration de domaine**.

Étape 3.4 - Téléchargez la base de données des utilisateurs.

Accédez à **Téléchargement utilisateur** pour récupérer la base de données utilisateur à partir du serveur AD.

Activez la case à cocher pour télécharger **les utilisateurs et les groupes de téléchargement** et définissez l'intervalle de temps sur la fréquence à laquelle le module Firepower contacte le serveur AD pour télécharger la base de données utilisateur.

Sélectionnez le groupe et ajoutez-le à l'option **Inclure** pour laquelle vous voulez configurer l'authentification. Par défaut, tous les groupes sont sélectionnés si vous ne choisissez pas d'inclure les groupes.

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Config	uration > Integration > <u>Realms</u>	
▶ Policies			
🕨 📕 Device Management	servertest		You have unsaved changes
🕨 🧒 Object Management			
🕨 🏠 Local	Enter a description		
ன System Information			
📑 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 V Hours	
🚟 Scheduling			
🕼 Import Export	E Download Now		
Troubleshooting	Available Groups	Groups to Include (0)	Groups to Exclude (0)
🔻 🍡 Integration			
Cisco CSI	Search by name	All available groups	None
🔏 Realms	A TAC		
🎍 Identity Sources			
Remote Management			
🛃 eStreamer			
		Add to	
		Include	
		Exclude	
💑 <u>D</u> evice Setup			
Firewall			
<u>R</u> emote 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)

Cliquez sur Store ASA Firepower Changes pour enregistrer la configuration du domaine.

Activez l'état du domaine et cliquez sur le bouton de téléchargement pour télécharger les utilisateurs et les groupes, comme illustré dans l'image.

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Configuration > Integration > Realms								
Policies									
🕨 📑 Device Management	Cisco CSI Realms Ide	antity Sources Rem	ote Managemer	eStreamer					
🕨 🧒 Object Management	cisco est incentits inc	intry bources interne	ote Hunagemen	it cotreamer		2.6			
🕨 🏠 Local						Compare	realms 😳	New	realm
ன System Information	Nama	Description	Tune	Base DN	Crown DN	Crown Attribute	Chata		1
📑 Updates	Name	Description	туре	base DN	Group DN	Group Attribute	State		
🖞 Licenses	servertest		AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tear	member		₽	🥒 🖣
🔻 💼 Tools								Downle	oad button
🗑 Backup Restore									
Scheduling									
Import Export					•				
Troubleshooting									
🔻 🔌 Integration									
Cisco CSI									

Étape 4. Configurez la stratégie d'identité.

Une stratégie d'identité effectue l'authentification des utilisateurs. Si l'utilisateur ne s'authentifie pas, l'accès aux ressources réseau est refusé. Cela applique le contrôle d'accès basé sur les rôles (RBAC) au réseau et aux ressources de votre entreprise.

Étape 4.1 Portail captif (Authentification active)

Active Authentication demande un nom d'utilisateur et un mot de passe dans le navigateur pour identifier une identité d'utilisateur afin d'autoriser toute connexion. Le navigateur authentifie l'utilisateur en présentant une page d'authentification ou s'authentifie silencieusement avec l'authentification NTLM. NTLM utilise le navigateur Web pour envoyer et recevoir des informations d'authentification. L'authentification active utilise différents types pour vérifier l'identité de l'utilisateur. Différents types d'authentification sont les suivants :

- 1. HTTP Basic : dans cette méthode, le navigateur demande des informations d'identification utilisateur.
- 2. NTLM : NTLM utilise les informations d'identification de la station de travail Windows et la négocie avec Active Directory à l'aide d'un navigateur Web. Vous devez activer l'authentification NTLM dans le navigateur. L'authentification utilisateur se produit de manière transparente sans demander d'informations d'identification. Il offre une expérience d'authentification unique aux utilisateurs.
- 3. **HTTP Negotiate :** Dans ce type, le système tente de s'authentifier à l'aide de NTLM, s'il échoue, le capteur utilise le type d'authentification HTTP Basic comme méthode de secours et invite une boîte de dialogue pour les informations d'identification de l'utilisateur.
- 4. Page de réponse HTTP : Ce type est similaire au type de base HTTP. Cependant, ici, l'utilisateur est invité à remplir l'authentification dans un formulaire HTML qui peut être personnalisé.

Chaque navigateur dispose d'une façon spécifique d'activer l'authentification NTLM et, par conséquent, vous pouvez suivre les directives du navigateur afin d'activer l'authentification NTLM.

Pour partager en toute sécurité les informations d'identification avec le capteur routé, vous devez installer un certificat de serveur auto-signé ou un certificat de serveur signé publiquement dans la stratégie d'identité.

Step 3. Generate the self-signed Certificate.

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

Accédez à Configuration > ASA FirePOWER Configuration > Policies > Identity Policy. Maintenant accédez à l'onglet Authentification active et dans l'option Certificat serveur, cliquez sur l'icône (+) et téléchargez le certificat et la clé privée que vous avez générés à l'étape précédente à l'aide d'openSSL, comme illustré dans l'image :

O O ASA FirePOWER Configurat	O O Configuration > ASA Firel	OWER Configuration > P	olicies > Identity Policy
 Policies Access Control Policy Intrusion Policy Files 	Default Identity Polic Identity Policy	/	You have unsaved changes
 SSL Actions Alerts Identity Policy DNS Policy Doty Policy Doty Compared the second se	Rules Active Authentication Server Certificate * None Port * 1025 Maximum login attempts * 3 Active Authentication Response Pa This page will be displayed if a user tri Authentication Type.	y () () () () () () () () () () () () () (Add Known Internal Certificate ? × Name: Server_Cert Certificate Data or, choose a file: Browse "BEGIN CERTIFICATE MIIDkDCCAvmgAwIBAgIJAPT h5TH1yBdMAAGCSqGSIb3DQEBBQUAMIGNMQswCQYD VQQEEwJUTJELMAKGATUECBMSOBEKAJQABUNABATCUUBTkdBTE9SRTEOMAwcGAIUE ChMFQ01TQ08xDDAKBgNVBASTAIRBQ2EaMBgGAIUEAxMRQDEuc2VydmVydGVzdCSj DozlazhBgkqhikGSw0BGQCHVGFKbWULQUPKBRVBAYTAKOMQswCQYDOWVYOQI EwJLQTESVMBAGAIUEBXMQkFGRbWULQUPKBRVBAYTAKOMQswCQYDVQQI EwJLQTESVMBAGAIUEBXMQkFGRbWULQUPKGFKbWULQUPKBRVDSVNDT2EMMAAGAIUE CMFQ01TQ08xDDAKBgNVBASTAIRBQ2EaMBgGAIUEAxMRQDEuc2VydmVydGVzdCSj EwJLQTESVMACAGIUEBXMQkFGRbWULQUSZVUZ2VUBKWDDSVNDTZEMMAAGAIUE CMFDQUFGCVGQUEFCQSZXUZZVUZXUZXUXUMUNWbVFTGWCZADSDQEI ARYUYWRtaWSAc2VydmVydGVzdCSjb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ Key or, choose a file: Browse
Troubleshooting Integration Cisco CSI Realms Identity Sources Remote Management Setteamer	System-provided Required when using Active Authenti	tation €	BEGIN RSA PRIVATE KEY Proc-Type: 4_ENCRYPTED DEK-Info: DES-EDE3-CBC, 83542C7C670DC917 mLeuBJX5T2apbAnOLR+sI,YAPqJKxiKigDjR/1RM3WDPK3WHnCvn7Rdwkvw3xbdBC G6u2y+J9wNIIC6sfq1QX21mbkp6LaX0fhJunUbktSjAKvmi7c1n00JipkfQj3 kHnebQGTTYWQPXXC0232qj2vHi52N2FD/4cz+a1RcSyekPEPpWJU67xKi2cy1/i LDF0FdF1gqALVNKtr0XY7X5cbpc2jBdUgKRAwcaSkyP+4zE/J77NVj tbYSoMw8uKR8BiJLT11/+YpWFT2b5x4g6j0n9UO4RosakCBKdQLIJwII49Gp0IP2 Encrypted, and the password is: Store ASA FirePOWER Changes Cancel
Site-to-Site VPN			Store ASA FirePOWER Changes Cancel

Cliquez maintenant sur **Ajouter une règle** pour donner un nom à la règle et choisissez l'action en tant qu'**Authentification active**. Définissez la zone source/destination, le réseau source/destination pour lequel vous voulez activer l'authentification utilisateur.

Accédez à l'onglet **Domaine et paramètres**. Sélectionnez le **domaine** dans la liste déroulante que vous avez configurée à l'étape précédente et sélectionnez le **type d'authentification** dans la liste déroulante qui convient le mieux à votre environnement réseau.

 Policies Access Control Policy Intrusion Policy Files SSL Active_Authentication Active_Authentication Enabled Insert into Category Standard Rules
Intrusion Policy Default I dentity Policy You have unsaved changes Intrusion Policy Add Rule ? × Intrusion Policy SSL Name Active_Authentication ? × Intrusion Alerts Name Active_Authentication Insert into Category > Standard Rules
Image: Solution Policy Add Rule ? × Image: Files Image: Solution Policy ? × Image: Solution Alerts Name Active_Authentication Image: Image: Solution Policy
Files SSL Name Active_Authentication Actions Alerts
SSL Name Active_Authentication Insert into Category Standard Rules Actions Alerts
S Actions Alerts
Light the servertest (AD) Action Passive Authentication V Realm: servertest (AD) Authentication Type: HTTP Basic Exclude HTTP User-Agents: None
DNS Policy
Source Management Zones Networks Ports Realm & Settings
▶ 💀 Object Management
▶
🗟 System Information 🛛 🗹 Use active authentication if passive authentication cannot identify user
i Updates
Tools Authentication Type HTTP Basic
😳 Backup Restore 🔰 Application Filters 🖒 Available Applications (83) Ĉ Exclude HTTP User-Agents (0)
Scheduling Search by name any any
Import Export
Troubleshooting
▼ [©] Integration Very Low 19 AdobeAIR Utu to Kue
Integration Very Low 19 AdobeAIR Image: Constraint of the second s
Integration Image: Wery Low 19 AdobeAIR Image: Cisco CSI Image: Low 40 Advanced Packaging Tool Image: Realms Image: Medium 11 AirPlay
▼ < Integration □ Very Low 19 □ AdobeAIR 0 Not or Note • C isco CSI □ □ Low 40 □ Advance Packaging Tool 0 • Realms □ □ Medium 11 □ AirPlay 0 • Identity Sources □ □ High 6 □ Anazon Instant Video 0
▼ < Integration □ Very Low 19 □ AdobeAIR ① Not or Kule • ◇ Cisco CSI □ □ Low 40 □ Advanced Packaging Tool ① • △ Realms □ △ Medium 11 □ AirPlay ① • △ Identity Sources □ ▲ High 6 □ Amazon Instant Video ③
▼ Integration Image: Very Low 19 Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR ◊ Cisco CSI Image: AddoeAIR Image: AddoeAIR Image: AddoeAIR
▼ < Integration Image: Very Low 19 Image: AddoeAIR Image: AddoeAIR

Étape 4.2 Configuration ASA pour Captive Portal.

Étape 1. Définissez le trafic intéressant qui sera redirigé vers Sourcefire pour inspection.

```
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
Étape 2. Configurez cette commande sur l'ASA afin d'activer le portail captif.
```

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

Astuce : captive-portal peut être activé globalement ou par interface.

Astuce : Assurez-vous que le port du serveur, TCP 1025, est configuré dans l'option de port de l'onglet Authentification active de la stratégie d'identité.

Étape 4.3 Authentification unique (authentification passive).

Dans l'authentification passive, lorsqu'un utilisateur de domaine se connecte et est en mesure d'authentifier la distance administrative, l'agent utilisateur Firepower interroge les détails du mappage utilisateur-IP à partir des journaux de sécurité d'AD et partage ces informations avec Firepower Module. Le module Firepower utilise ces informations afin d'appliquer le contrôle d'accès.

Pour configurer la règle d'authentification passive, cliquez sur **Ajouter une règle** pour donner un nom à la règle, puis choisissez l'**action** comme **authentification passive**. Définissez la zone source/destination, le réseau source/destination pour lequel vous voulez activer l'authentification utilisateur.

Accédez à la **Domaine et paramètres**. Sélectionnez le **Domaine** dans la liste déroulante que vous avez configurée à l'étape précédente.

Vous pouvez choisir la méthode de retour en arrière comme **authentification active si** l'authentification passive ne peut pas identifier l'identité de l'utilisateur, comme illustré dans l'image :

O O ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Policies > Identity Policy	
Vertical Policies		
Access Control Policy	Default Identity Policy	You have unsaved change
Intrusion Policy	Add Bule	2 ×
Files		
SSL Actions Alasts	Name Passive Authentication	
Actions Alerts		
DNS Policy	Action Passive Authentication	Basic Exclude HTTP User-Agents: None
Device Management	Zones Networks Ports	Realm & Settings
🕨 🧒 Object Management		Kouin a bettings
► 🏠 Local	Realm * servertest (AD)	
ன System Information		
📑 Updates	Use active authentication if passive authentication cannot identify user	
🔛 Licenses		
V 💼 Tools		
Backup Restore		
Scheduling		
🕼 Import Export		
Troubleshooting		
Integration		
A Realms		
Remote Management		
estreamer		
	* Required Field	
		Add Cancel

Cliquez maintenant sur **Store ASA Firepower Changes** pour enregistrer la configuration de la stratégie d'identité.

Étape 5. Configurez la stratégie de contrôle d'accès.

Accédez à Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy.

Cliquez sur la **stratégie d'identité** (dans le coin supérieur gauche), sélectionnez la stratégie d'identification que vous avez configurée à l'étape précédente dans la liste déroulante et cliquez sur **OK**, comme illustré dans cette image.

O O ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy								
Policies									
📳 Access Control Policy	ASA ASA FirePOWER								
Intrusion Policy									
💾 Files	Default Allow All Traffic								
E SSL	Enter a description								
X Actions Alerts									
Lentity Policy									
DNS Policy									
Device Management	🔀 📙 Status: Access Control policy out-of-date on device								
🕨 🧑 Object Management									
Local	Identity Policy: None SSL Policy: None								
ன System Information	Pulsa Couvily Intelligence LITTE Researce								
📑 Updates	Kules Security Intelligence http://www.ceu								
🔛 Licenses	General Settings // Transport/Network Layer Preprocessor Settings	Ø							
V 💼 Tools	Identity Policy								
3 Backup Restore	Maximum URL characters to AN header when tracking connections	No							
Scheduling	Allow an Interactive Block Default Identity Policy	ß							
🕼 Import Export	infancement Seturgs								
Troubleshooting	Retry URL cache miss look	Disabled							
Integration	Inspect traffic during policy analyzes the second								
Cisco CSI	Performance Settings	li l							

Cliquez sur **Ajouter une règle** pour ajouter une nouvelle règle, accédez à **Utilisateurs** et sélectionnez les utilisateurs pour lesquels la règle de contrôle d'accès sera appliquée, comme illustré dans cette image, puis cliquez sur **Ajouter**.

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Co	nfiguration > Policies > Access Control P	Policy	
▼				
Access Control Policy	ASA ASA FirePOWER			
Intrusion Policy				
🖺 Files	Default Allow All Traffic			You have unsaved changes
🔒 SSL				
🔯 Actions Alerts	Enter a description			
🚨 Identity Policy	Add Rule			? ×
DNS Policy				
🕨 🔜 Device Management	Name	Enabled	Insert below rule	✓ 1
🕨 🧒 Object Management	Action Allow	✓ IPS: no policies Variables: n/a Fi	les: no inspection Logaina: no logai	na
▶ 🏠 Local				
System Information	Zones Networks Users Applicatio	ons Ports 🔺 URLs 🔺 ISE Attributes		Inspection Logging Comments
📑 Updates	Available Realms	Available Users	Selecter	
Licenses			Selected	
Tools	Search by name or value	Search by name or value	A serve	ertest/TAC
Backup Restore	() Special Identities	servertest/*		
Scheduling	() servertest	A TAC		
		sunil		
Troubleshooting		Sum -		
	1		Add to Rule	
& Realms				
Jentity Sources				
Remote Management				
Restreamer				
A Device Setup				Add Cancel

Cliquez sur **Modifications apportées au pare-feu ASA du magasin** pour enregistrer la configuration de la stratégie de contrôle d'accès.

Étape 6. Déployez la stratégie de contrôle d'accès.

Vous devez déployer la stratégie de contrôle d'accès. Avant d'appliquer la stratégie, vous verrez une mention Politique de contrôle d'accès obsolète sur le module. Pour déployer les modifications sur le capteur, cliquez sur **Déployer** et choisissez **l'option Déployer les modifications FirePOWER** puis cliquez sur **Déployer** dans la fenêtre contextuelle.

Note: Dans la version 5.4.x, pour appliquer la stratégie d'accès au capteur, cliquez sur Apply ASA FirePOWER Changes.

Note: Naviguez jusqu'à Monitoring > ASA Firepower Monitoring > Task Status. Assurez-vous que la tâche doit être terminée en appliquant la modification de configuration.

Étape 7. Surveiller les événements utilisateur.

Accédez à **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventil**, pour surveiller le type de trafic utilisé par l'utilisateur.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Accédez à **Analysis > Users** afin de vérifier le type d'authentification/d'authentification utilisateur/mappage utilisateur-IP/règle d'accès associé au flux de trafic.

Connectivité entre le module Firepower et l'agent utilisateur (authentification passive)

Le module Firepower utilise le port TCP 3306, afin de recevoir les données du journal d'activité de l'utilisateur de l'agent utilisateur.

Afin de vérifier l'état du service du module Firepower, utilisez cette commande dans le FMC.

admin@firepower:~\$ netstat -tan | grep 3306 Exécutez la capture de paquets sur le FMC afin de vérifier la connectivité avec l'Agent utilisateur.

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

Connectivité entre FMC et Active Directory

Le module Firepower utilise le port TCP 389 afin de récupérer la base de données utilisateur à partir de Active Directory.

Exécutez la capture de paquets sur le module Firepower pour vérifier la connectivité avec Active Directory.

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

Assurez-vous que les informations d'identification de l'utilisateur utilisées dans la configuration du domaine disposent de privilèges suffisants pour récupérer la base de données utilisateur d'AD.

Vérifiez la configuration du domaine et assurez-vous que les utilisateurs/groupes sont téléchargés et que le délai d'expiration de la session utilisateur est configuré correctement.

Accédez à Surveillance de l'état des tâches de surveillance ASA Firepower et assurez-vous que le téléchargement des tâches par les utilisateurs/groupes s'est terminé correctement, comme illustré dans cette image.

Connectivité entre ASA et système d'extrémité (authentification active)

authentification active, assurez-vous que le certificat et le port sont correctement configurés dans la stratégie d'identité du module Firepower et dans ASA (commande captive-portal). Par défaut, ASA et le module Firepower écoutent sur le port TCP 885 pour l'authentification active.

Afin de vérifier les règles actives et leur nombre de coups, exécutez cette commande sur l'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, port=1025, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=identity
Output Table:
L2 - Output Table:
```

```
L2 - Input Table:
```

Configuration des politiques et déploiement des politiques

Assurez-vous que les champs Domaine, Type d'authentification, Agent utilisateur et Action sont configurés correctement dans Stratégie d'identité.

Assurez-vous que la stratégie d'identité est correctement associée à la stratégie de contrôle d'accès.

Naviguez jusqu'à Monitoring > ASA Firepower Monitoring > Task Status et assurez-vous que le déploiement de la stratégie se termine correctement.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques Cisco Systems
- <u>Configurer l'intégration Active Directory avec Firepower Appliance pour l'authentification</u> <u>unique et l'authentification captive du portail</u>