Active Directory-Integration mit ASDM für Single-Sign-On und Captive Portal Authentication (On-Box-Management) konfigurieren

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Schritt 1: Konfigurieren Sie den FirePOWER User Agent für die einmalige Anmeldung. Schritt 2: Integrieren Sie das FirePOWER-Modul (ASDM) in den User Agent. Schritt 3: Integrieren Sie FirePOWER in Active Directory. Schritt 3.1 Erstellen Sie den Bereich. Schritt 3.2 Fügen Sie die IP-Adresse/den Hostnamen des Verzeichnisservers hinzu. Schritt 3.3 Ändern Sie die Bereichskonfiguration. Schritt 3.4 Laden Sie die Benutzerdatenbank herunter. Schritt 4: Konfigurieren Sie die Identitätsrichtlinie. Schritt 5: Konfigurieren Sie die Zugriffskontrollrichtlinie. Schritt 6: Bereitstellen der Zugriffskontrollrichtlinie. Schritt 7: Überwachen von Benutzerereignissen Überprüfen Verbindung zwischen FirePOWER-Modul und Benutzer-Agent (passive Authentifizierung) Verbindungen zwischen FMC und Active Directory Verbindung zwischen ASA und Endsystem (aktive Authentifizierung) Richtlinienkonfiguration und Richtlinienbereitstellung Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die Konfiguration der Captive Portal Authentication (Active Authentication) und Single-Sign-On (Passive Authentication) für das FirePOWER-Modul mithilfe von ASDM (Adaptive Security Device Manager).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der ASA-Firewall (Adaptive Security Appliance) und des ASDM
- Fachwissen zum FirePOWER-Modul
- Light Weight Directory Service (LDAP)
- FirePOWER UserAgent

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 5.4.1 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Captive Portal Authentication (Captive Portal) oder Active Authentication (Aktive Authentifizierung) fordert eine Anmeldeseite und Benutzeranmeldeinformationen auf, damit ein Host auf das Internet zugreifen kann.

Die Single-Sign-On- oder Passive-Authentifizierung ermöglicht eine nahtlose Authentifizierung von Benutzern für Netzwerkressourcen und Internetzugriff, ohne dass die Anmeldeinformationen der Benutzer mehrfach eingegeben werden müssen. Die Single-Sign-On-Authentifizierung kann entweder über den FirePOWER User Agent oder die NTLM Browser-Authentifizierung erfolgen.

Hinweis: Captive Portal Authentication, ASA sollte sich im Routing-Modus befinden.

Hinweis: Der Captive Portal-Befehl ist in der ASA-Version 9.5(2) und später verfügbar.

Konfigurieren

Schritt 1: Konfigurieren Sie den FirePOWER User Agent für die einmalige Anmeldung.

In diesem Artikel wird erläutert, wie Sie den FirePOWER User Agent auf dem Windows-Computer konfigurieren:

Installation und Deinstallation von Sourcefire User Agent

Schritt 2: Integrieren Sie das FirePOWER-Modul (ASDM) in den User Agent.

Melden Sie sich bei ASDM an, navigieren Sie zu Configuration > ASA FirePOWER Configuration

> Integration > Identity Sources und klicken Sie auf die Option User Agent. Nachdem Sie auf die Option User Agent geklickt haben, konfigurieren Sie die IP-Adresse des User Agent-Systems. auf Hinzufügen klicken, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	○ ○ O Configuration > ASA FirePOWER Configuration > Integration > Identity Sources	
Policies		
🕨 🐻 Device Management	Cisco CST Realms Identity Sources Remote Management eStreamer	
🕨 🧒 Object Management	Cisto coa realinas Adeinte Sources Reinote Planagement estreamer	-
🕨 🏠 Local	You have unsaved changes Cancel Save	
🔄 System Information		1
📑 Updates		
🔡 Licenses	Identity Sources	
🔻 💼 Tools	Service Type Nona I Identify Condense Engine I How Assert	
🗑 Backup Restore	None vaenuty services crigine User Agent	
Scheduling	🔘 New Agent	
Import Export	Host Name/IP Address Licer Agent 2 X	
Troubleshooting		
🔻 🍡 Integration		
Cisco CSI	Host Name/IP Address 192.168.10.11	
🔏 Realms		
🍛 Identity Sources		
🔯 Remote Management	Add Cancel	
📴 eStreamer		

Klicken Sie auf die Schaltfläche Speichern, um die Änderungen zu speichern.

Schritt 3: Integrieren Sie Firepower in Active Directory.

Schritt 3.1 Erstellen Sie den Bereich.

Melden Sie sich beim ASDM an, wählen Sie **Configuration > ASA FirePOWER Configuration >** Integration > Realms (Konfiguration > ASA FirePOWER-Konfiguration > Integration > Bereiche) aus. Klicken Sie auf Neuen Bereich hinzufügen.

Name und Beschreibung: Geben Sie einen Namen bzw. eine Beschreibung an, um den Bereich eindeutig zu identifizieren.

Typ: AD

AD Primary Domain: Domain name of Active Directory (NETBIOS-Name).

Verzeichnisbenutzername: Geben Sie den <*Benutzernamen*> an.

Verzeichniskennwort: Geben Sie das < Kennwort> an.

Basis-DN: Domäne oder spezifischer OU-DN, von dem aus das System eine Suche in der LDAP-Datenbank startet.

Gruppen-DN: Geben Sie die Gruppen-DNs an.

Gruppenattribut: Geben Sie die Option Member aus der Dropdown-Liste an.

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ Config	uration > A	SA Fire	POWER Conf	iguratio	n > Integration	> <u>Re</u>	alms					
Policies													
🕨 📑 Device Management	Cisco CSI	Realms	Ident	tity Sources	Rem	ote Managemer	nt I	eStreamer					
🕨 🧑 Object Management	0.000 0.01			,		oto nanagenio.		concurren			D.C.	. 0	
▶ 🏠 Local											Compare re	ealms 🙂	New realm
System Information	Name			Description		Type	Bas	e DN	Group DN	Group At	ttribute	State	
📑 Updates		-							•	_			
Licenses		Add New	v Realn	n					? ×				
V Tools													
Schoduling		Name *		S	ervertest								
Import Export		Descripti	ion										
		Tuno			_		~						
 Integration 		Type •		A	J								
Cisco CSI		AD Prima	ary Doma	ain * se	ervertest.c	om		ex: domain.com					
🔏 Realms		Directory	y Usernar	me * se	ervertest\a	ıdmin		ex: user@domain					
凝 Identity Sources		Directory	v Passwo	ord *									
Remote Management													
📝 eStreamer		Base DN	*	d	c=serverte	st,dc=com		ex: ou=user,dc=cis	co,dc=com				
		Group D	N *	CI	=TAC,ou	=Security-Team,dc	=serv	ex: ou=group,dc=c	isco,dc=com				
		Group At	ttribute	м	ember		~						
		* Requir	ed Field										
								ОК	Cancel				

Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Dieser Artikel hilft Ihnen, die Werte für Basis-DN und Gruppen-DN zu ermitteln.

Identifizieren von Active Directory-LDAP-Objektattributen

Schritt 3.2 Fügen Sie die IP-Adresse/den Hostnamen des Verzeichnisservers hinzu.

Um die IP/Hostname des AD-Servers anzugeben, klicken Sie auf Verzeichnis hinzufügen.

Hostname/IP-Adresse: Konfigurieren Sie die IP-Adresse/den Hostnamen des AD-Servers.

Port: Geben Sie die Active Directory-LDAP-Portnummer an (Standard 389).

Verschlüsselung/SSL-Zertifikat: (optional) Informationen zur Verschlüsselung der Verbindung zwischen FMC- und AD-Server finden Sie in diesem Artikel:

<u>Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication Over</u> <u>SSL/T...</u>

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA EiroPOWER Configuration > Integration > Pealms	
Policies		
🕨 📕 Device Management	servertest	
🕨 🕨 😡 Object Management	Enter a description	
🕨 🏠 Local		
ன System Information		
📑 Updates	Directory Realm Configuration User Download	
🔢 Licenses		
🔻 💼 Tools		
🗑 Backup Restore	URL (Hostname/IP Address and Port)	Encryption
Scheduling	Add directory 2	×
🕼 Import Export	Add directory	~
J Troubleshooting	Hostname / IP 192 168 10 11	
🔻 🍡 Integration	Address	
Cisco CSI	Port 389	
a Realms		
ldentity Sources	Encryption STARTILS LDAPS None	
🔞 Remote Management	SSL Certificate 🗸 🕥	
🔯 eStreamer		
	OK Test Cancel	

Klicken **Test** um die Verbindung von FMC mit dem AD-Server zu überprüfen. Klicken Sie jetzt auf **OK**, um die Konfiguration zu speichern.

Schritt 3.3 Ändern Sie die Bereichskonfiguration.

Um die Integrationskonfiguration des AD-Servers zu ändern und zu überprüfen, navigieren Sie zu **Realm Configuration**.

Schritt 3.4 Laden Sie die Benutzerdatenbank herunter.

Navigieren Sie zu User Download, um die Benutzerdatenbank vom AD-Server abzurufen.

Aktivieren Sie das Kontrollkästchen zum Herunterladen von **Benutzern und Gruppen herunterladen** und definieren Sie das Zeitintervall darüber, wie häufig das FirePOWER-Modul AD-Server zum Herunterladen von Benutzerdatenbank kontaktiert.

Wählen Sie die Gruppe aus, und fügen Sie sie zur **Include-**Option hinzu, für die Sie die Authentifizierung konfigurieren möchten. Standardmäßig sind alle Gruppen ausgewählt, wenn Sie die Gruppen nicht einschließen möchten.

O O 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		
Eccal			
System Information	Disastan Dealer Configuration User Bounds		
Updates	Directory Realm Configuration User Downlo		
Elicenses			
Rackup Postoro			
Schoduling	Begin automatic download at 12 V AM V Ame	erica/New York Repeat Every 24 Y Hours	
	Download Now		
Troubleshooting			
 Integration 	Available Groups 🖒	Groups to Include (0)	Groups to Exclude (0)
Cisco CSI	Search by name	All available groups	None
🔏 Realms	A TAC		
ldentity Sources			
💿 Remote Management			
📴 eStreamer			
		Add to	
		Include	
		Add to	
		Exclude	
Bevice Setup			
Firewall			
<u> R</u> emote Access VPN			
Site-to-Site VPN		Enter User Inclusion Ad	Enter User Exclusion Add
ASA FirePOWER Configur			
Device <u>M</u> anagement		Store ASA FirePOWER Changes Cancel	

Klicken Sie auf Store ASA FirePOWER Changes um die Realm-Konfiguration zu speichern.

Aktivieren Sie den Realmstatus, und klicken Sie auf die Download-Schaltfläche, um die Benutzer und Gruppen herunterzuladen, wie im Bild gezeigt.

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > /	ASA Fir	rePOWER Config	uration	1 > Integration	> <u>Realms</u>						
Policies												
🕨 🜄 Device Management	Cisco CST Realms	Ide	entity Sources	Rem	ote Manageme	eStreamer						
🕨 🧒 Object Management	tibes est iteams		since, sources	TCOTT.	oternanagemen			2.6				
A Local								Comp	pare realms	s 😳 I	New r	realm
🔄 System Information	Name		Description		Tune	Page DN	Crown DN	Crown Attribute		inte l		
📑 Updates	Name		Description		туре	base DN	Group DN	Group Attribute	50	late		
🗏 Licenses	servertest				AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tear	n member		< </td <td>₽</td> <td>🥔 🖣</td>	₽	🥔 🖣
🔻 💼 Tools										_	Downlo	oad button
🗑 Backup Restore												
Scheduling												
🕼 Import Export							•					
Troubleshooting												
🔻 🐚 Integration												
Cisco CSI												
🔏 Realms												

Schritt 4: Konfigurieren Sie die Identitätsrichtlinie.

Eine Identitätsrichtlinie führt die Benutzerauthentifizierung durch. Wenn sich der Benutzer nicht authentifiziert, wird der Zugriff auf Netzwerkressourcen verweigert. Dadurch wird eine rollenbasierte Zugriffskontrolle (RBAC) für das Netzwerk und die Ressourcen Ihres Unternehmens erzwungen.

Schritt 4.1 Captive Portal (Active Authentication).

Bei der aktiven Authentifizierung werden Benutzername und Kennwort im Browser benötigt, um eine Benutzeridentität zu identifizieren und eine Verbindung zuzulassen. Der Browser authentifiziert Benutzer entweder durch Anzeige der Authentifizierungsseite oder authentifiziert sich stumm durch NTLM-Authentifizierung. NTLM verwendet den Webbrowser, um Authentifizierungsinformationen zu senden und zu empfangen. Die aktive Authentifizierung verwendet verschiedene Typen, um die Identität des Benutzers zu überprüfen. Folgende Authentifizierungstypen sind verfügbar:

- 1. HTTP Basic: Bei dieser Methode fordert der Browser zur Eingabe von Benutzeranmeldeinformationen auf.
- 2. NTLM: NTLM verwendet Windows-Workstation-Anmeldeinformationen und handelt sie mithilfe eines Webbrowsers über Active Directory aus. Sie müssen die NTLM-Authentifizierung im Browser aktivieren. Die Benutzerauthentifizierung erfolgt transparent, ohne dass Sie zur Eingabe von Anmeldeinformationen aufgefordert werden. Es bietet eine einmalige Anmeldung für Benutzer.
- HTTP Negotiate (HTTP-Aushandlung): Bei diesem Typ versucht das System, sich mithilfe von NTLM zu authentifizieren. Wenn dies fehlschlägt, verwendet der Sensor den HTTP Basic-Authentifizierungstyp als Fallbackmethode und fordert ein Dialogfeld für Benutzeranmeldeinformationen auf.
- 4. HTTP-Antwortseite: Dies ähnelt dem grundlegenden HTTP-Typ. Hier wird der Benutzer jedoch aufgefordert, die Authentifizierung in einem HTML-Formular auszufüllen, das angepasst werden kann.

Jeder Browser verfügt über eine spezielle Möglichkeit, die NTLM-Authentifizierung zu aktivieren. Daher können Sie die Browser-Richtlinien befolgen, um die NTLM-Authentifizierung zu aktivieren.

Um die Anmeldeinformationen sicher für den gerouteten Sensor freizugeben, müssen Sie entweder ein selbstsigniertes Serverzertifikat oder ein öffentlich signiertes Serverzertifikat in der Identitätsrichtlinie installieren.

```
Step 3. Generate the self-signed Certificate.
```

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

Navigieren Sie zu Konfiguration > ASA FirePOWER Configuration > Policies > Identity Policy.. Navigieren Sie jetzt zur Registerkarte Active Authentication (Aktive Authentifizierung), und klicken Sie in der Option Server Certificate auf das Symbol (+). und laden Sie das Zertifikat und den privaten Schlüssel hoch, die Sie im vorherigen Schritt mit openSSL generiert haben, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > F	Policies > Identity Policy
V Dolicies		
The second secon	Default Identity Policy	You have unsaved changes
▶ Intrusion Policy	Derudic ruenercy roney	
Tiles	Identity Policy	
A SSL		
Actions Alerts		Add Known Internal Certificate ? ×
& Identity Policy		
DNS Policy		Name: Server_Cert
Device Management	Rules Active Authentication	Cartificate Data or choose a file:
🕨 🧑 Object Management		
🕨 🏠 Local	Server Certificate * None	BEGIN CERTIFICATE MTIDkDCCAymoAwIBAnTJAPTn5TIH1yBdMA0GCSnGSTh3DOEBBOLIAMTGNMOswCOYD
🔄 System Information		VQQGEwJJTjELMAkGA1UECBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UE
📑 Updates	1025	(88 ChMFQ0ITQ08xDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5j b20_LAAbB_bbb//20_000051/FC6LbM/001010271020000000000000000000000000000
🔡 Licenses	Maximum login attempts * 3	0 ODE1MzE0NVoXDTI2MDUxNiE1MzE0NVovaY0xCzAIBaNVBAYTAkIOMOswCOYDVOOI
🔻 💼 Tools		EwJLQTESMBAGA1UEBxMJQkFOR0FMT1JFMQ4wDAYDVQQKEwVDSVNDTzEMMAoGA1UE
🗑 Backup Restore	Active Authentication Response Page	CxMDVEFDMRowGAYDVQQDExFDQS5zZXJ2ZXJ0ZXN0LmNvbTEjMCEGCSqGSIb3DQEJ
Scheduling	This page will be displayed if a user triggers an identity rule with HTT Authentication Type	P P
💽 Import Export	Addiction Type.	Key or, choose a file: Browse
Troubleshooting	System-provided 💙	REGIN RSA PRIVATE KEY
🔻 🍡 Integration		Proc-Type: 4,ENCRYPTED
Cisco CSI	* Required when using Active Authentication	DEK-Info: DES-EDE3-CBC,B3542C7C670DC917
🔏 Realms		mLeuBJX5T2apbAnOLR+sLYAPaJKxiXiaDiR/1RM3WDPK3WHnCvn7Rdwkvw3xbdBC
🚣 Identity Sources		G6u2y+J9wNIIC6sfg4ItjX2Imbkp6LaX0fhlJunUbktSjAKvmi7cIno0JipkfQi3
Remote Management		kHhebQGTTYWQFXXCC923qj2vitlSZN2FD/4cz+aIRc5yekPEPpWJU67kKi2cy1/i
🛃 eStreamer		tbYSoMw8uKR8BIjLTJ1/+YpWFT2bBx4q6iOn9UO4RosakCBKdQLIJwIi49GpOIP2
		Encrypted, and the password is:
A Device Setup		Store ASA FirePOWER Changes Cancel
ASDM-IDM		
- Irewald		
🥂 Remote Access VPN		
ASA FirePOWER Configur		Store ASA FirePOWER Changes Cancel
· · ·		

Klicken Sie jetzt auf **Regel hinzufügen**, um der Regel einen Namen zu geben, und wählen Sie die Aktion als **aktive Authentifizierung aus**. Definieren Sie die Quell-/Zielzone, das Quell-/Zielnetzwerk, für das Sie die Benutzerauthentifizierung aktivieren möchten.

Navigieren Sie zur Registerkarte **Bereich und Einstellungen**. Wählen Sie den **Bereich** aus der Dropdown-Liste aus, die Sie im vorherigen Schritt konfiguriert haben, und wählen Sie den **Authentifizierungstyp** aus der Dropdown-Liste aus, der Ihrer Netzwerkumgebung am besten entspricht.



Schritt 4.2 ASA-Konfiguration für Captive Portal

Schritt 1: Definieren Sie den interessanten Datenverkehr, der zur Überprüfung an Sourcefire umgeleitet wird.

```
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 Schritt 2: Konfigurieren Sie diesen Befehl auf der ASA, um das Captive Portal zu aktivieren.

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

Tipp: Captive-Portal kann global oder pro Schnittstellenbasis aktiviert werden.

Tipp: Stellen Sie sicher, dass der Server-Port TCP 1025 in der Port-Option der Registerkarte Active Authentication (Aktive Authentifizierung) der Identitätsrichtlinie konfiguriert ist.

Schritt 4.3 Einmalige Anmeldung (passive Authentifizierung).

Wenn sich ein Domänenbenutzer bei der passiven Authentifizierung anmeldet und das AD authentifizieren kann, fragt der FirePOWER User Agent die Benutzer-IP-Zuordnungsdetails aus den Sicherheitsprotokollen von AD ab und gibt diese Informationen an das FirePOWER-Modul weiter. Das FirePOWER-Modul verwendet diese Details, um die Zugriffskontrolle durchzusetzen.

Um die passive Authentifizierungsregel zu konfigurieren, klicken Sie auf **Regel hinzufügen**, um der Regel einen Namen zuzuweisen, und wählen Sie dann **Aktion** als **Passive Authentication (Passive Authentifizierung)**. Definieren Sie die Quell-/Zielzone, das Quell-/Zielnetzwerk, für das Sie die

Benutzerauthentifizierung aktivieren möchten.

Navigieren Sie zum **Bereich und Einstellungen** Registerkarte. Wählen Sie **Bereich** aus der Dropdown-Liste aus, die Sie im vorherigen Schritt konfiguriert haben.

Hier können Sie die Fallback-Methode als **aktive Authentifizierung** auswählen, **wenn die passive Authentifizierung die Benutzeridentität nicht identifizieren kann**, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Policies > Identity Policy	
Vertication Policies		
🚦 Access Control Policy	Default Identity Policy	You have unsaved change
Intrusion Policy		
💾 Files	Add Rule	? ×
🔒 SSL		
🔯 Actions Alerts	Name Passive_Authentication 🗹 Enabled Insert below rule 💙 1	
🚨 Identity Policy	Action Passive Authentication Realm: servertest (AD) Authentication Type: HTTP Basic Exclude HTTP User-Agents:	
DNS Policy		
🕨 📑 Device Management	Zones Networks Ports	Realm & Settings
🕨 🧒 Object Management		j ····································
🕨 🏠 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	
	Ad	Id Cancel

Klicken Sie jetzt auf **Store ASA FirePOWER Changes** um die Konfiguration der Identitätsrichtlinie zu speichern.

Schritt 5: Konfigurieren Sie die Zugriffskontrollrichtlinie.

Navigieren Sie zu Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy.

Klicken Sie auf die **Identitätsrichtlinie** (in der linken oberen Ecke), wählen Sie die Identitätsrichtlinie aus, die Sie im vorherigen Schritt konfiguriert haben, und klicken Sie auf **OK**, wie in diesem Bild gezeigt.

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	
🔒 SSL	Enter a description	
🔯 Actions Alerts	Litter & description	
🚨 Identity Policy		
DNS Policy		
🕨 📷 Device Management	📝 📘 Status: Access Control policy out-of-date on device	
🕨 🧑 Object Management		
► 🏠 Local	Identity Policy: None SSL Policy: None	
🔄 System Information		
📑 Updates	Rules Security Intelligence HTTP Responses Advanced	
🔡 Licenses	General Settings	la l
🔻 💼 Tools	Identity Policy 2 X	
🔄 Backup Restore	Maximum URL characters to AN header when tracking connections	No
Scheduling	Allow as Interactive Black	
健 Import Export	hancement Settings	l d l
HTroubleshooting	Retry URL cache miss look	Disabled
🔻 🍡 Integration	Revert to Defaults	
Cisco CSI	Performance Settings	Ø

Klicken Sie auf **Regel hinzufügen** Um eine neue Regel hinzuzufügen, navigieren Sie zu **Benutzer** die Benutzer auswählen, für die die Zugriffskontrollregel erzwungen wird, wie in diesem Bild gezeigt, und auf **Hinzufügen** klicken.

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	Berdare Anow An Hame			
🔯 Actions Alerts	Enter a description			
🚨 Identity Policy	Add Rule			? ×
DNS Policy				
🕨 🔜 Device Management	Name	Enabled	Insert below rule	▼ 1
🕨 🧔 Object Management	Action Allow	Y IPS: no policies Variables: n/a Fi	les: no inspection Logging: no loggin	20
🕨 🏠 Local	Allow			9
🔄 System Information	Zones Networks Users Application	ons Ports 🔺 URLs 🔺 ISE Attributes) (Inspection Logging Comments
📑 Updates			Calastad	
🔛 Licenses	Available Realms	Available Users	Selected	Users (1)
🔻 🧰 Tools	Search by name or value	Search by name or value	serve 🛃	rtest/TAC
Backup Restore	G Special Identities	servertest/*		
Scheduling	servertest			
💽 Import Export				
Troubleshooting		a sunii		
 Integration 			Add to Rule	
Cisco CSI				
A Realms				
and the sources				
estreamer				
				Add Cancel
Pevice Setup				

Klicken Sie auf **ASA FirePOWER-Änderungen speichern** um die Konfiguration der Zugriffskontrollrichtlinie zu speichern.

Schritt 6: Bereitstellen der Zugriffskontrollrichtlinie.

Sie müssen die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, wird auf dem Modul eine veraltete Anzeige "Zugriffskontrollrichtlinie" angezeigt. Um die Änderungen am Sensor bereitzustellen, klicken Sie auf **Bereitstellen** und wählen Sie die **Option FirePOWER-**Änderungen bereitstellen. Klicken Sie anschließend im Popup-Fenster auf **Bereitstellen**.

Hinweis: In Version 5.4.x müssen Sie auf Apply ASA FirePOWER Changes klicken, um die Zugriffsrichtlinie auf den Sensor anzuwenden.

Hinweis: Navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Task Status. Stellen Sie sicher, dass die Anwendung der Konfigurationsänderung abgeschlossen sein muss.

Schritt 7: Überwachen von Benutzerereignissen

Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing**, um die Art des vom Benutzer verwendeten Datenverkehrs zu überwachen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Navigieren Sie zu **Analyse > Benutzer,** um die Benutzerauthentifizierungs-/Authentifizierungstyp-/Benutzer-IP-Zuordnungs-/Zugriffsregel zu überprüfen, die dem Datenverkehrsfluss zugeordnet ist.

Verbindung zwischen FirePOWER-Modul und Benutzer-Agent (passive Authentifizierung)

Das FirePOWER-Modul verwendet den TCP-Port 3306, um Benutzeraktivitätsprotokolldaten vom Benutzer-Agent zu empfangen.

Um den Dienststatus des FirePOWER-Moduls zu überprüfen, verwenden Sie diesen Befehl im FMC.

admin@firepower:~\$ netstat -tan | grep 3306

Führen Sie die Paketerfassung auf dem FMC aus, um die Verbindung mit dem Benutzer-Agent zu überprüfen.

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

Verbindungen zwischen FMC und Active Directory

Das FirePOWER-Modul verwendet den TCP-Port 389, um die Benutzerdatenbank aus dem Active-Verzeichnis abzurufen.

Führen Sie die Paketerfassung für das FirePOWER-Modul aus, um die Verbindung mit dem Active Directory zu überprüfen.

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

Stellen Sie sicher, dass die in der Realm-Konfiguration verwendeten Anmeldeinformationen über ausreichende Berechtigungen zum Abrufen der Benutzerdatenbank des AD verfügen.

Überprüfen Sie die Realm-Konfiguration, und stellen Sie sicher, dass die Benutzer/Gruppen heruntergeladen und das Timeout für die Benutzersitzung korrekt konfiguriert werden.

Navigieren Sie zu Monitoring ASA FirePOWER Monitoring Task Status (Status der ASA FirePOWER-Überwachungsaufgabe), und stellen Sie sicher, dass der Download der Task-Benutzer/-Gruppen erfolgreich abgeschlossen wurde, wie in diesem Bild gezeigt.

Verbindung zwischen ASA und Endsystem (aktive Authentifizierung)

aktive Authentifizierung: Stellen Sie sicher, dass das Zertifikat und der Port in der FirePOWER-Modul-Identitätsrichtlinie und ASA (Captive-Portal-Befehl) korrekt konfiguriert sind. Standardmäßig lauschen ASA- und FirePOWER-Module den TCP-Port 885 für die aktive Authentifizierung ab.

Führen Sie diesen Befehl auf der ASA aus, um die aktiven Regeln und deren Trefferanzahl zu überprüfen.

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
```

```
L2 - Output Table:
L2 - Input Table:
Last clearing of hits counters: Never
```

Richtlinienkonfiguration und Richtlinienbereitstellung

Stellen Sie sicher, dass die Felder Bereich, Authentifizierungstyp, Benutzeragent und Aktion in der Identitätsrichtlinie korrekt konfiguriert sind.

Stellen Sie sicher, dass die Identitätsrichtlinie der Zugriffskontrollrichtlinie korrekt zugeordnet ist.

Navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Aufgabenstatus, und stellen Sie sicher, dass die Richtlinienbereitstellung erfolgreich abgeschlossen wurde.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation Cisco Systems
- Konfigurieren der Active Directory-Integration mit der FirePOWER-Appliance für die Single-Sign-On- und Captive Portal-Authentifizierung