



ダイナミック ファイアウォールの設定

- [ダイナミック ファイアウォールの設定方法 \(1 ページ\)](#)
- [ダイナミック属性フィルタの作成 \(15 ページ\)](#)

ダイナミック ファイアウォールの設定方法

このトピックは、「[ダイナミック ファイアウォールについて](#)」で説明されている [ダイナミック ファイアウォール](#) を設定するための概念とオプションを理解するのに役立ちます。

process_summary

ダイナミック ファイアウォールは、Cisco Secure Firewall Management Center にユーザー信頼情報を提供する Cisco Identity Intelligence と (Cisco ISE などの) アイデンティティソースを統合します。

1. ユーザー信頼情報を収集するように Cisco Identity Intelligence を設定します。
2. サポートされている Cisco Secure Firewall Management Center アイデンティティソースを設定します。
3. サポートされているアイデンティティレルムを設定します。
4. 動的属性コネクタ をイネーブルにします。
5. [ダイナミック ファイアウォール](#) を設定します。

process_workflow

次に、[ダイナミック ファイアウォール](#) を設定する方法の概要を示します。

1. 所有者ロールを持つ Duo ユーザーとして、Cisco アイデンティティ インテリジェンス テナントをプロビジョニングします。

[Cisco Identity Intelligence テナントのプロビジョニング](#)で説明されているように、Duo Advantage からテナントをプロビジョニングできます。

2. Cisco アイデンティティ インテリジェンス で、API 統合を作成し、その情報を使用してダイナミック ファイアウォール をセットアップします。

シスコでは、Cisco アイデンティティ インテリジェンス を使用してネットワーク内のユーザーおよびデバイスリスク情報を特定しています。

Cisco アイデンティティ インテリジェンス の詳細については、[ハウツーガイド](#)を参照してください。

このタスクの詳細については、「[アイデンティティ インテリジェンス の必要な情報の取得 \(4 ページ\)](#)」を参照してください。

3. (Microsoft Azure AD レルムのみ) アイデンティティ インテリジェンス で、Microsoft Entra ID 統合を作成します。

詳細については、『[Microsoft Entra ID \(Azure AD\) Data Integration](#)』を参照してください。

4. アイデンティティ ソースを作成します (アイデンティティ ソースがすでにある場合は、次のステップに進みます)。

これは、次のいずれかの方法で実行できます。

- [\[ダイナミックファイアウォールの設定 \(Configure Dynamic Firewall\)\]](#) ダイアログボックスに、アイデンティティ ソースの設定を開始するための [\[設定 \(Configure\)\]](#) リンクが表示されます。
- [\[システム \(System\)\]](#) (⚙️) > [\[統合 \(Integration\)\]](#) > [\[アイデンティティ ソース \(Identity Sources\)\]](#) をクリックします。

アイデンティティ ソースの詳細については、以下を参照してください。

- [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティ ソースの設定方法](#)
- [pxGrid クラウドアイデンティティ ソースの設定方法 \(ISE 3.3 以前\)](#)
- [pxGrid クラウドアイデンティティ ソースの設定方法 \(ISE 3.4 以降\)](#)

5. アイデンティティ レルムを作成します。

次のレルムをサポートしています。

- [LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成](#)
Microsoft AD のみがサポートされています。LDAP レルムはサポートされていません。
- [パッシブ認証用の Azure AD \(SAML\) レルムの作成](#)

6. 動的属性コネクタ をイネーブルにします。

動的属性コネクタ は、ダイナミック ファイアウォール を使用するために必要です。これにより、アイデンティティ ソースをアイデンティティ インテリジェンス と統合して、ユーザーアクティビティに関する洞察を強化できます。

「[ダイナミック属性コネクタの有効化](#)」を参照してください。

7. ダイナミック ファイアウォール インスタンスを作成します（ダイナミック ファイアウォール インスタンスがすでにある場合は、次のステップに進みます）。
[統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] の順にクリックし、**[ダイナミックファイアウォールの設定 (Configure Dynamic Firewall)]** をクリックします。
[ダイナミック ファイアウォール インスタンスを作成します。 \(6 ページ\)](#) を参照してください。
8. アイデンティティソースを Cisco アイデンティティ インテリジェンスに関連付けます。
[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(7 ページ\)](#) を参照してください。
9. システム定義フィルタを表示します。
ダイナミック属性フィルタは以下を区別するために作成します。
 - 信頼できないデバイス
 - 信頼できるデバイス
 - 信頼できないユーザー
 - 疑わしいユーザー
「[ダイナミック属性フィルタの作成 \(15 ページ\)](#)」で説明されているように、これらのダイナミック属性フィルタを編集または置換できます。
10. システム定義のアクセス制御ルールを表示します。
次のルールを使用して、Dynamic Firewall Policy という（または同様の）名前のアクセスコントロール ポリシーを作成します。
 - 任意の送信元ネットワークから任意の宛先ネットワークへの信頼できないユーザーをブロックします。
 - 任意の送信元ネットワークから任意の宛先ネットワークへの疑わしいユーザーを監視します。
 - 任意の送信元ネットワークから任意の宛先ネットワークへの信頼できないデバイスをブロックします。
「[システム作成のアクセスコントロールポリシーの表示と編集 \(14 ページ\)](#)」で説明されているように、アクセスコントロールポリシーとアクセス制御ルールを編集または削除します。

動的属性コネクタの有効化

このタスクでは、Cisco Secure Firewall Management Center で動的属性コネクタを有効にする方法について説明します。動的属性コネクタは、クラウドネットワーキング製品のオブジェクト

を Cisco Secure Firewall Management Center のアクセス制御 のルールで使用できるようにする統合です。

手順

ステップ1 Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ2 [統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] をクリックします。

ステップ3 [有効 (Enabled)] にスライドします。

ステップ4 動的属性コネクタ が有効になっている間、メッセージが表示されます。

エラーが発生した場合は、再試行してください。エラーが続く場合には、[Cisco TAC](#)に連絡してください。

アイデンティティ インテリジェンス の必要な情報の取得

このタスクでは、ダイナミック ファイアウォールでアイデンティティ インテリジェンス をセットアップするために必要なすべての情報を提供する API クライアントの作成方法について説明します。

すでに API クライアントがあり、次のすべての値がわかっている場合は、この手順をスキップして「」に進むことができます。

- Client ID
- API URL
- トークン URL
- クライアントのシークレット (Client Secret)

始める前に

ダイナミック ファイアウォール と統合するには、アイデンティティ インテリジェンス で API クライアント統合を作成する必要があります。

API クライアント統合について知っておく必要がある値の中に、クライアントシークレットがあります。これは、API クライアントを作成するときのみ表示されます。このため、最初に API 統合を作成する必要があります。

API クライアント統合の作成の詳細については、「[Public API](#)」を参照してください。

手順

ステップ1 [アイデンティティ インテリジェンス テナント](#) にログインします。

ステップ2  ([統合 (Integrations)]) をクリックします。

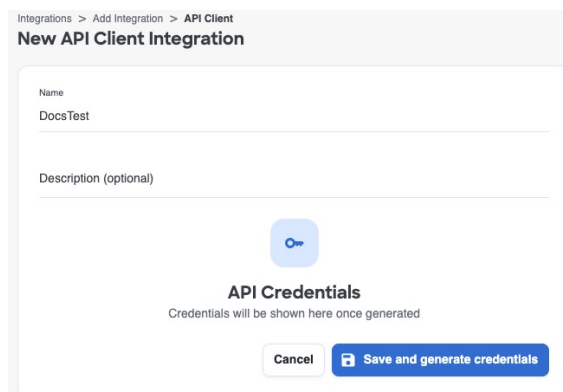
ステップ 3 [統合の追加 (Add Integration)] をクリックします。

ステップ 4 次のページの [APIクライアント (API Clients)] で、[APIクライアントの追加 (Add API Client)] をクリックします。

ステップ 5 [名前 (Name)] とオプションの [説明 (Description)] を入力します。

ステップ 6 [保存してログイン情報を生成 (Save and Generate Credentials)] をクリックします。

次の図は例を示しています。



Integrations > Add Integration > API Client

New API Client Integration

Name
DocsTest

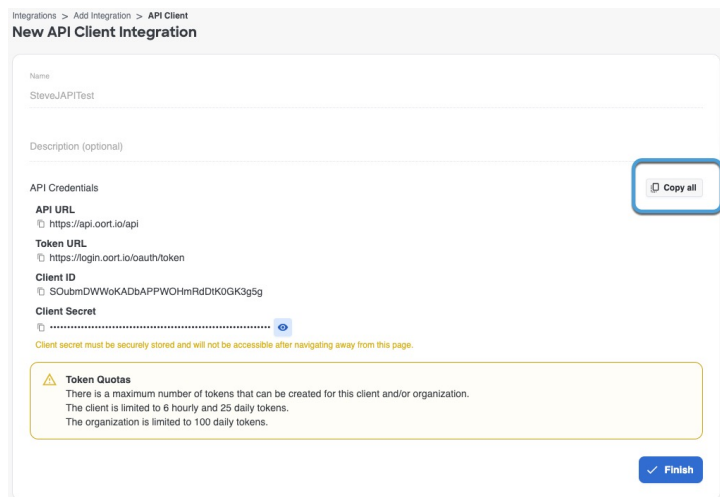
Description (optional)

Copy

API Credentials
Credentials will be shown here once generated

Cancel Save and generate credentials

ステップ 7 次の図に示すように、次のページで [すべてコピー (Copy all)] をクリックします。



Integrations > Add Integration > API Client

New API Client Integration

Name
Steve.JAPITest

Description (optional)

API Credentials **Copy all**

API URL
https://api.oort.io/api

Token URL
https://login.oort.io/oauth/token

Client ID
S0ubmDWWoKADbAPPWOHmRdDK0GK3g5g

Client Secret
.....

Client secret must be securely stored and will not be accessible after navigating away from this page.

Token Quotas
There is a maximum number of tokens that can be created for this client and/or organization.
The client is limited to 6 hourly and 25 daily tokens.
The organization is limited to 100 daily tokens.

Finish

ステップ 8 後で使用できるようにログイン情報を保存します。

ステップ 9 [終了 (Finish)] をクリックします。

ダイナミック ファイアウォールのアイデンティティソースおよびレルムの作成

ダイナミック ファイアウォールを設定する前に、サポートされているアイデンティティレルムとアイデンティティソースを設定する必要があります。

アイデンティティレルムの設定

次のアイデンティティレルムがサポートされています。

- [LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成](#)
Microsoft AD のみがサポートされています。LDAP レルムはサポートされていません。
- [パッシブ認証用の Azure AD \(SAML\) レルムの作成](#)

アイデンティティソースの設定

次のアイデンティティソースがサポートされています。

- オンプレミスの Cisco ISE : [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)
- 単一または複数の Cisco ISE クラスター :
 - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
 - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

ダイナミック ファイアウォール インスタンスを作成します。


このタスクでは、アイデンティティソースとアイデンティティ インテリジェンス 間の関連付けであるダイナミック ファイアウォールの新しいインスタンスを作成する方法について説明します。

始める前に

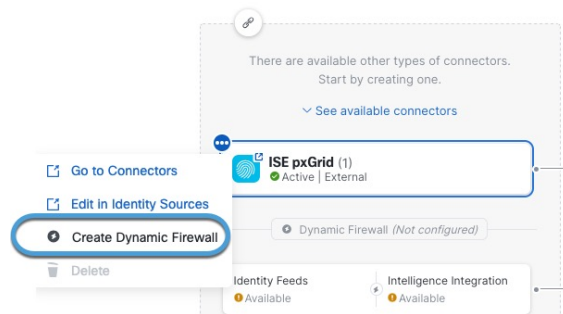
次のことをすべて行います。

- 「」の説明に従って 動的属性コネクタ を有効にします。
- アイデンティティソースを作成します。
 - オンプレミスの Cisco ISE : [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)
 - 単一または複数の Cisco ISE クラスター :
 - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
 - [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

手順

- ステップ 1** まだログインしていない場合は、Cisco Secure Firewall Management Center にログインします。
- ステップ 2** [統合 (Integrations)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] の順にクリックします。
- ステップ 3** アイデンティティソースの名前の横にある  をクリックし、ダイナミック ファイアウォール を追加します。

次の図は例を示しています。



(注)

アイデンティティソースが表示されない場合は、続行する前に作成します。

- [Cisco Identity Services Engine \(Cisco ISE\) のアイデンティティソースの設定方法](#)。
- [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.3 以前\)](#)
- [pxGrid クラウドアイデンティティソースの設定方法 \(ISE 3.4 以降\)](#)

- ステップ 4** [ダイナミックファイアウォールの作成 (Create Dynamic Firewall)] をクリックします。
- ステップ 5** 「[アイデンティティソースとアイデンティティ インテリジェンスの関連付け](#)」に進みます。

アイデンティティ インテリジェンス とアイデンティティソースとの関連付け

このタスクでは、ユーザーとデバイスの信頼評価を Cisco Secure Firewall Management Center に提供する アイデンティティ インテリジェンス にアイデンティティソースを関連付ける方法について説明します。

詳細については、『[User Trust Level](#)』を参照してください。

始める前に

手順を開始する前に、次の点を確認してください。

- 「[ダイナミック ファイアウォールについて](#)」に記載されている、アイデンティティレルム、アイデンティティソース、およびアイデンティティ インテリジェンス が連携する仕組みを理解している。
- 「[ダイナミック ファイアウォール インスタンスを作成します。 \(6 ページ\)](#)」で説明されているタスクを完了している。

手順

ステップ 1 [ダイナミック ファイアウォール インスタンスの作成](#)から開始します。

ステップ 2 次のページの左列で、アイデンティティソースをクリックします。右列で[Cisco Identity Intelligence] チェックボックスをオンにして、ユーザーとデバイスのリスクを含むユーザーインテリジェンスを追加します。

次の図は例を示しています。

The screenshot shows the 'Dynamic Firewall' configuration interface. It is divided into two main columns: 'User identity feeds' and 'Intelligence integration'. In the 'User identity feeds' column, the 'ISE pxGrid On-Prem' option is selected with a radio button. In the 'Intelligence integration' column, the 'Cisco Identity Intelligence' option is checked with a blue checkmark. A 'Next' button is visible at the bottom right of the configuration area. The interface also includes a progress indicator on the left with three steps: '1 Associate an identity source with an identity intelligence integration', '2 View system-defined filters', and '3 View system-defined access control policy rules'.

ステップ 3 [Next] をクリックします。

ステップ 4 [アイデンティティ インテリジェンス の設定 \(9 ページ\)](#) に進みます。

アイデンティティ インテリジェンス の設定

このタスクでは、ユーザーとデバイスのリスクレーティングを Cisco Secure Firewall Management Center に提供する アイデンティティ インテリジェンス にアイデンティティソースを関連付ける方法について説明します。

始める前に

「[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(7 ページ\)](#)」で説明されているタスクを完了します。

手順

- ステップ 1 「[アイデンティティ インテリジェンス とアイデンティティソースとの関連付け \(7 ページ\)](#)」で説明されているタスクを完了します。
- ステップ 2 [Cisco Identity Intelligence] チェックボックスをオンにした場合は、「[アイデンティティ インテリジェンス の必要な情報の取得 \(4 ページ\)](#)」の説明に従って、アイデンティティ インテリジェンス について見つけた情報を入力します。

次の図は例を示しています。

The screenshot shows the 'Dynamic Firewall' configuration interface. The current step is '2 Configure CII connector'. The form contains the following fields and controls:

- Name***: CII
- CII API URL***: https://.../lo/api
- Token URL***: https://.../token
- Client ID***: AgC...
- Client Secret***: [Redacted]
- Pull interval (hours)**: 24
- EXCLUSION LIST**: A toggle switch is turned off. Below it, it says 'No exclusions for this connector.'
- Buttons: 'Test', 'Back', and 'Next'.

- ステップ 3 (オプション) アイデンティティ インテリジェンス に対し、特定のユーザーセットを信頼できるとみなす場合は、[除外リスト (Exclusion List)] を [有効なスライダ (Slider enabled)] () にスライドします。

username@domain.com 形式で1行に1つのユーザー名を入力します。このリストのユーザーは、アイデンティティ インテリジェンス によって信頼できるとみなされます。

- ステップ 4 [テスト (Test)] をクリックします。

テストが成功した場合にのみ、次の手順に進みます。

エラーが表示された場合は、アイデンティティインテリジェンスのすべての値を確認して再試行します。

ステップ5 [Next] をクリックします。

ステップ6 [システム定義フィルタの表示 \(10 ページ\)](#) に進みます。

システム定義フィルタの表示

このタスクでは、ユーザーとデバイスのリスクレーティングを Cisco Secure Firewall Management Center に提供する Cisco アイデンティティインテリジェンスにアイデンティティソースを関連付ける方法について説明します。

始める前に

「[アイデンティティインテリジェンスの設定](#)」を参照してください。

手順



ステップ1 次の図に示すように、システムにはシステム定義のダイナミック属性フィルタのセットが表示されます。

Dynamic Firewall ? ×


- 1 Associate an identity source with an identity intelligence integration
- 2 Configure CII connector
- 3 **View system-defined filters**
- 4 View system-defined access control policy rules

We're creating the following system-defined filters for you. Click [help](#) for more information.

4 dynamic attributes filters

Name	Query
Untrusted_Device	(PostureStatus eq 'NonCompliant') OR ((MdmRegistered eq 'true') AND (MdmCo... 
Trusted_Device	(PostureStatus eq 'Compliant') OR ((MdmRegistered eq 'true') AND (MdmCo... 
Untrusted_User	TrustScore eq 'UNTRUSTED'
Questionable_User	TrustScore eq 'QUESTIONABLE'

[Back](#) [Next](#)

ステップ 2 システムが作成したフィルタを表示します。任意の行の  をクリックしてフィルタを展開すると、フィルタを表示して詳細を確認できます。

ステップ 3 [Next] をクリックします。

ステップ 4 [システム定義のアクセス制御ルールの表示 \(11 ページ\)](#) に進みます。

システム定義のアクセス制御ルールの表示

このタスクでは、ダイナミック ファイアウォールによって作成されたアクセス制御ルールについて説明します。

始める前に

[システム定義フィルタの表示 \(10 ページ\)](#) を参照してください。

手順

ステップ 1 システムで作成されたアクセス制御ルールを表示します。

次の図は例を示しています。

The screenshot shows a 'Dynamic Firewall' configuration window with a progress indicator on the left. Step 4, 'View system-defined access control policy rules', is active. Below the progress indicator is a table of rules:

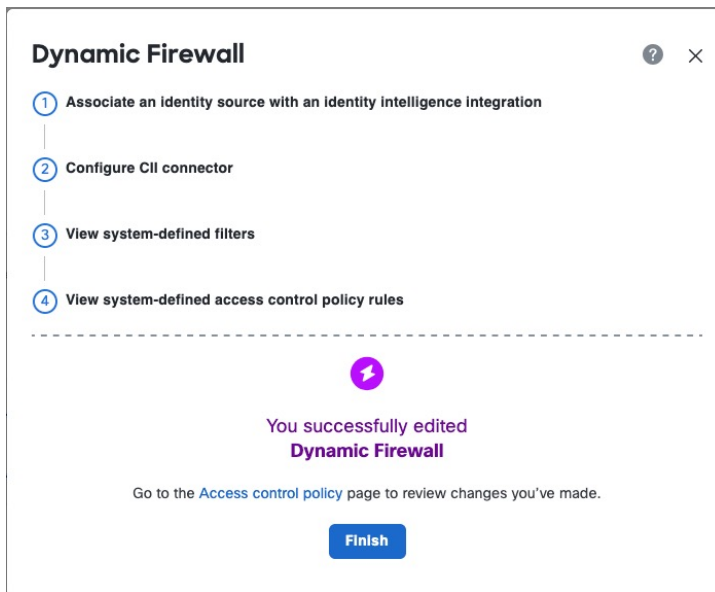
Rule Name	Action	Dynamic Attributes
Block_Untrusted_User	Block	SRC: Untrusted_User, DST: ANY
Inspect_Questionable_User	Monitor	SRC: Questionable_User, DST: ANY
Block_Untrusted_Device	Block	SRC: Untrusted_Device, DST: ANY

At the bottom of the window are three buttons: 'Skip', 'Back', and 'Next'.

ステップ 2 次のオプションのいずれかを選択します。

- これらのアクセス制御ルールの作成をスキップするには、[スキップ (Skip)] をクリックします。独自の設定はいつでも作成できます。
- [次へ (Next)] をクリックし、前の図に示すルールを使用して **Dynamic Firewall Policy** という名前のアクセスコントロールポリシーを作成します。
- システムが作成したフィルタに戻るには、[戻る (Back)] をクリックします。

ステップ 3 アクセス制御ルールの作成が成功した場合、[次へ (Next)] をクリックすると次のページが表示されます。




ユーザー除外リストの編集

(オプション) アイデンティティインテリジェンスに対し、特定のユーザーを信頼できるユーザーとして扱うように指示できます。

始める前に

「[ダイナミック ファイアウォール インスタンスを作成します。 \(6 ページ\)](#)」の説明に従って [ダイナミック ファイアウォール](#) を設定します。

手順

- ステップ 1** まだ Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ 2** [統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] をクリックします。
- ステップ 3** アイデンティティソースの名前の横にある  をクリックします。
- ステップ 4** [CII除外リストの編集 (Edit CII Exclusion List)] をクリックします。

次のダイアログボックスが表示されます。

Edit CII Exclusion List

EXCLUSION LIST

Enter each user name on a separate line

Enter one or more users to exclude from filters. These users will not be treated as untrusted users.
User names are case-sensitive.

Cancel OK

ステップ 5 指定のフィールドに、username@domain.com の形式で 1 行に 1 つのユーザー名を入力して Enter を押し、別のユーザー名を入力します。

各ユーザー名は アイデンティティ インテリジェンス によって信頼できるとみなされます。

システム作成のアクセス コントロール ポリシーの表示と編集

このトピックでは、システムで作成されたアクセス制御ルールとアクセス コントロール ポリシーを編集する方法について説明します。最初は、ポリシーはデバイスに関連付けられていませんが、それを使用する場合は、デバイスの追加、ルールの変更、ルールの順序変更、またはルールの削除を行えます。

始める前に

「[システム定義のアクセス制御ルールの表示 \(11 ページ\)](#)」で説明されている操作を完了させます。

手順

ステップ 1 まだ Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ2 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [アクセス制御 (Access Control)] をクリックします。

ステップ3 [Dynamic Firewall Policy] (または同様の名前) という名前のポリシーの横にある [編集 (Edit)] (🔗) をクリックします。

次の図に、サンプルのアクセス コントロール ポリシーを示します。

	Name	Action	Source			Destination		
			Zones	Networks	Dynamic Attributes	Zones	Networks	Ports
Mandatory 3 rules (1 - 3)								
<input type="checkbox"/>	1 Inspect_Questionable...	Monitor	Any	Any	Questionable_User	Any	Any	Any
<input type="checkbox"/>	2 Block_Untrusted_Device	Block	Any	Any	Untrusted_Device	Any	Any	Any
<input type="checkbox"/>	3 Block_Untrusted_User	Block	Any	Any	Untrusted_User	Any	Any	Any
Default (No rules)								

このアクセスコントロールポリシーでは、疑わしいユーザーを監視するルールセットのみがログに記録されることに注意してください。ロギング設定を調整するには、「[アクセスコントロールポリシーのロギング設定](#)」を参照してください。

ステップ4 次のいずれかを実行します。

- デバイスでアクセス コントロール ポリシーをターゲットにする：[アクセス コントロール ポリシーへのデバイスの割り当て](#)。
- ポリシーを編集する（ロギングの追加など）：[アクセス コントロール ポリシーの管理](#)。
- アクセス制御ルールを編集する：[アクセス制御ルールの管理](#)。
- 詳細ポリシーオプションを設定する：[アクセス コントロール ポリシーの詳細設定](#)。
- このアクセスコントロールポリシーに他のポリシーを関連付ける：[アクセス制御への他のポリシーの関連付け](#)。

ダイナミック属性フィルタの作成

を使用して定義する動的属性フィルタは、アクセス コントロール ポリシーで使用できるダイナミックオブジェクトとして Cisco Secure Firewall Management Center で公開されます。たとえば、財務部門の AWS サーバーへのアクセスを、Microsoft Active Directory で定義された財務グループのメンバーのみに制限できます。

手順

ステップ1 Cisco Secure Firewall Management Center にログインします。

ステップ2 [統合 (Integration)] > [ダイナミック属性コネクタ (Dynamic Attributes Connector)] > [コネクタ (Connectors)] をクリックします。

ステップ3 次のいずれかを実行します。

- 新しいフィルタの追加：追加 (+) をクリックします。
- フィルタの編集または削除：その他 (⋮) をクリックしてから、行の末尾にある [編集 (Edit)] または [削除 (Delete)] をクリックします。

ステップ4 次の情報を入力します。

項目	説明
[名前 (Name)]	アクセス コントロール ポリシーおよび Cisco Secure Firewall Management Center オブジェクトマネージャ ([外部属性 (External Attributes)] > [ダイナミックオブジェクト (Dynamic Object)]) で動的フィルタを (ダイナミックオブジェクトとして) 識別するための一意の名前。
コネクタ (Connector)	リストから、使用するコネクタの名前をクリックします。
クエリ (Query)	[追加 (Add)] (+) をクリックします。

ステップ5 クエリを追加するには、次の情報を入力します。

項目	説明
キー (Key)	リストからキーをクリックします。キーはコネクタから取得されます。
操作 (Operation)	次のいずれかをクリックします。 <ul style="list-style-type: none"> • キーを値に正確に一致させるには、[等しい (Equals)]。 • 値のいずれかの部分が一致する場合に、キーを値に一致させるには、[含む (Contains)]。
値 (Value)	[任意 (Any)] または [すべて (All)] をクリックし、リストから1つ以上の値をクリックします。[別

項目	説明
	の値を追加 (Add another value)] をクリックして、クエリに値を追加します。

ステップ 6 [プレビューを表示 (Show Preview)] をクリックして、クエリによって返されたネットワークまたは IP アドレスのリストを表示します。

ステップ 7 完了したら、[保存 (Save)] をクリックします。

ステップ 8 (オプション) Cisco Secure Firewall Management Center のダイナミックオブジェクトを確認します。

- a) 最低限でもネットワーク管理者ロールを持つユーザーとして Cisco Secure Firewall Management Center にログインします。
- b) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [外部属性 (External Attributes)] > [ダイナミックオブジェクト (Dynamic Objects)] をクリックします。
作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。