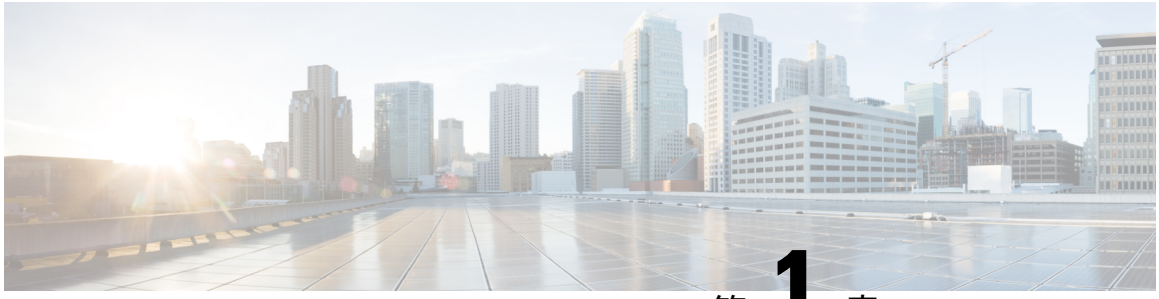
ダイナミック ファイアウォール ソリューション ガイド

最終更新：2026 年 5 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

ダイナミック ファイアウォール について

以下のトピックでは、ダイナミック ファイアウォール に関する一般情報を提供します。

ダイナミック ファイアウォール について

これまで、Cisco Secure Firewall Management Center は、Microsoft Active Directory、パッシブ ID エージェント、Cisco Identity Services Engine（Cisco ISE） などの設定されたアイデンティティ ソースからのみユーザーに関する情報を収集していました。この情報には通常、ユーザー名、グループ、IP アドレスが含まれていました。

ダイナミック ファイアウォール を使用すると、アイデンティティ ソースが提供する情報に Cisco アイデンティティ インテリジェンス からのユーザー リスク スコアを追加できるため、常に最新のユーザー ポスチャとリスクに基づいてポリシーを設定することが可能です。ユーザー アイデンティティとインテリジェンスを組み合わせ、その情報をレポートおよびアクセス コントロール ポリシーで使用できるようにします。

ダイナミック ファイアウォール を使用するには、次の条件を満たしている必要があります。

- アイデンティティ インテリジェンス テナントがあること。

  『Duo Identity Security with Cisco Identity Intelligence』を参照してください。

- 動的属性コネクタ の有効化
- アイデンティティ ソースをセットアップしていること。
  - Cisco Identity Services Engine（Cisco ISE）
  - pxGrid クラウド

    pxGrid クラウド は同じフィードでアイデンティティとポスチャを組み合わせます。

    詳細については、「What is pxGrid?」を参照してください。

認証情報に加えて、Cisco ISE と pxGrid クラウド は次の情報を提供できます。

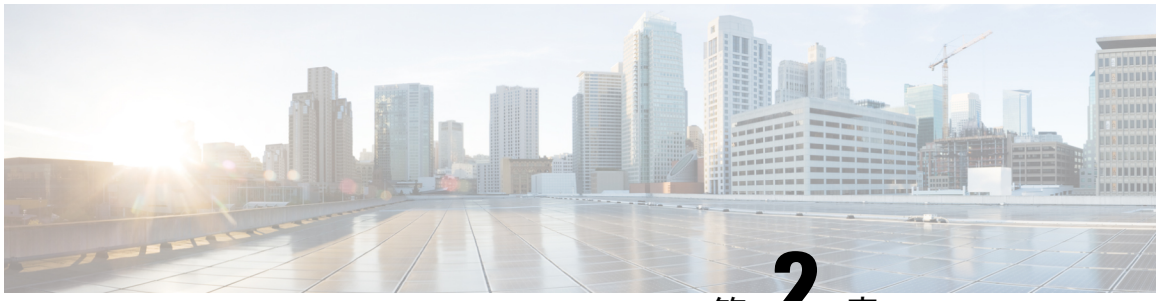
ダイナミック ファイアウォールについて

- SGT Exchange Protocol over TCP（SXP）バインディングおよびディレクトリセッション情報（必要に応じて）。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
- ポスチャおよびモバイルデバイス管理のコンプライアンス。詳細については、「Compliance」を参照してください。

- アイデンティティレルムをセットアップしていること。
  - 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
  - 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は、認証情報（ログイン、ログアウト）とポスチャを提供します。アイデンティティソースは、必要に応じて SXP バインディングおよびセッションディレクトリ情報も提供できます。

アイデンティティレルムは 、ユーザー、グループ、および IP アドレス情報を提供します。



第 2 章

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

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 （1 ページ）」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 （6 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。 （8 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 （9 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 （17 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 （16 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にのみ表示されます。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。

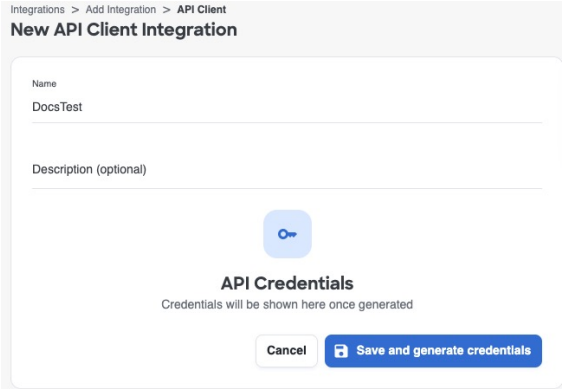
ステップ 3 [統合の追加（Add Integration）] をクリックします。

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。

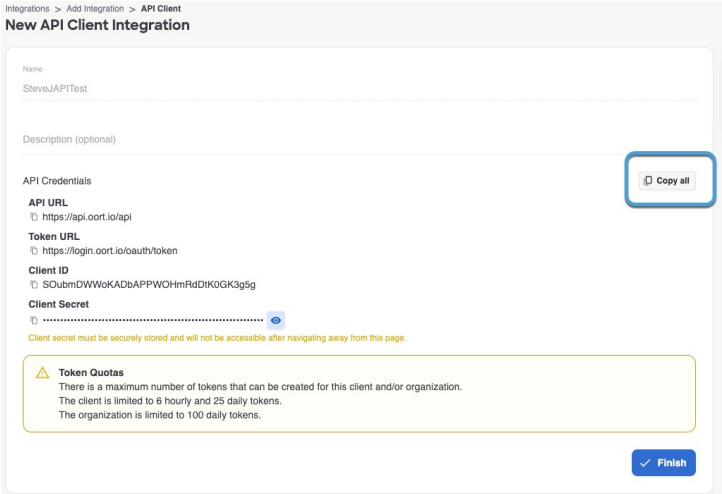
ステップ 5 [名前（Name）] とオプションの [説明（Description）] を入力します。

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。



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。



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）

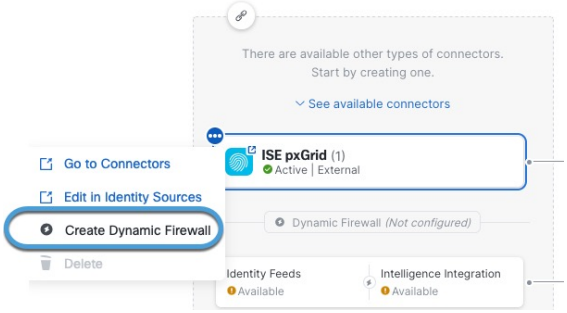
手順

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。

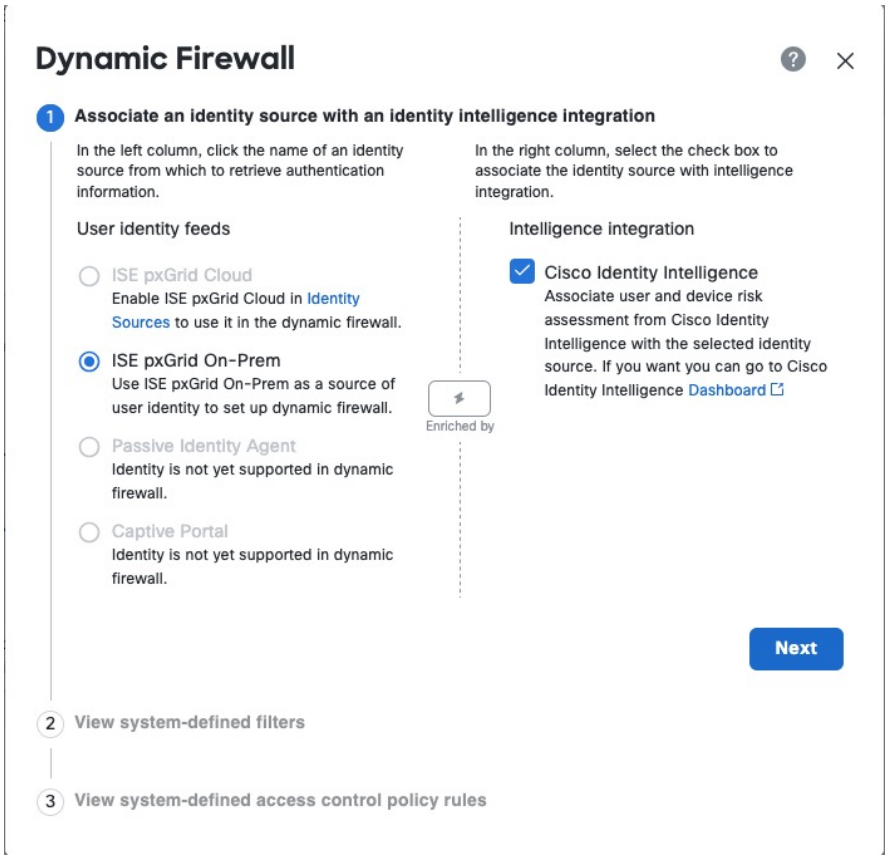
- 「ダイナミック ファイアウォール について （1 ページ）」に記載されている、アイデンティティレルム、アイデンティティソース、および アイデンティティ インテリジェンスが連携する仕組みを理解している。
- 「ダイナミック ファイアウォール インスタンスを作成します。 （8 ページ）」で説明されているタスクを完了している。

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。



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 （11 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

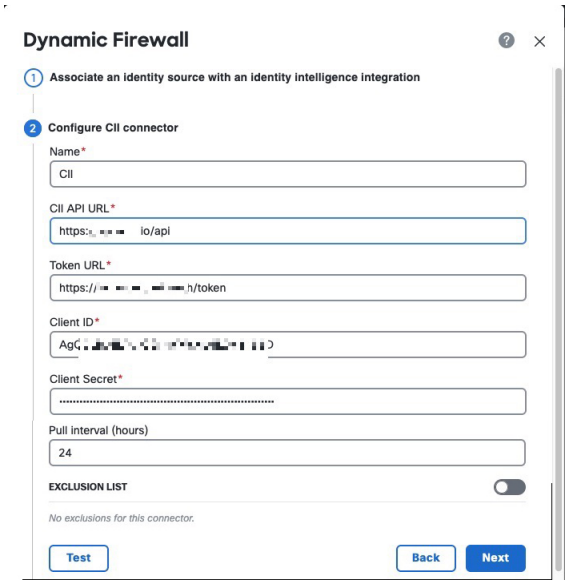
「アイデンティティ インテリジェンス とアイデンティティ ソースとの関連付け （9ページ）」で説明されているタスクを完了します。

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 （9 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 （6 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。



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 （12 ページ）に進みます。

システム定義フィルタの表示

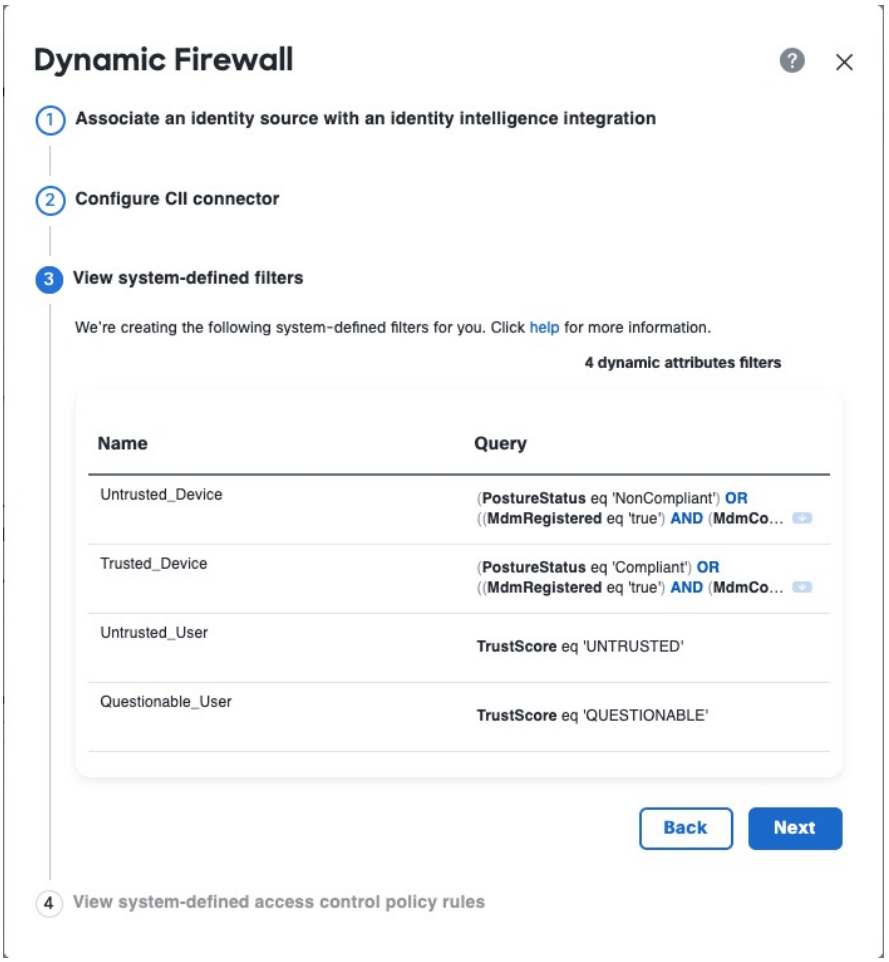
このタスクでは、ユーザーとデバイスのリスクレーティングを Cisco Secure Firewall Management Center に提供する Cisco アイデンティティインテリジェンスにアイデンティティソースを関連付ける方法について説明します。

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。



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 （13 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。

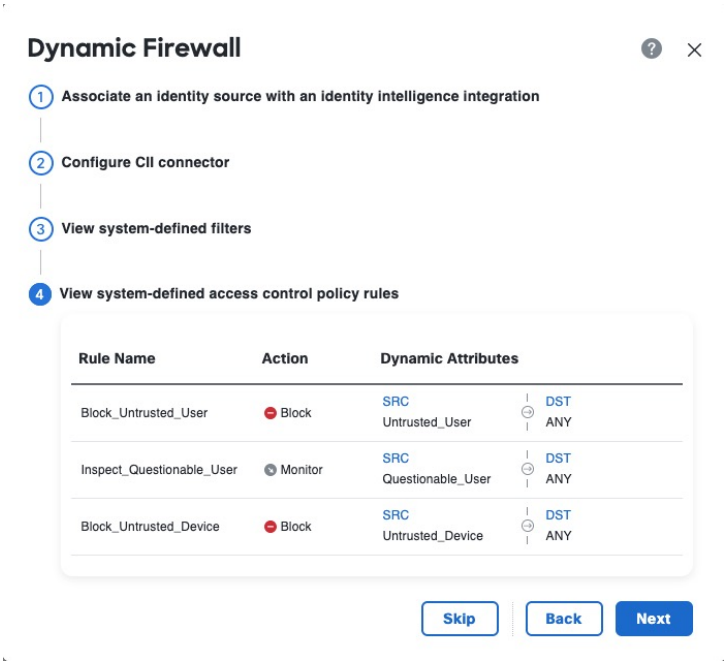
始める前に

システム定義フィルタの表示 （12 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。

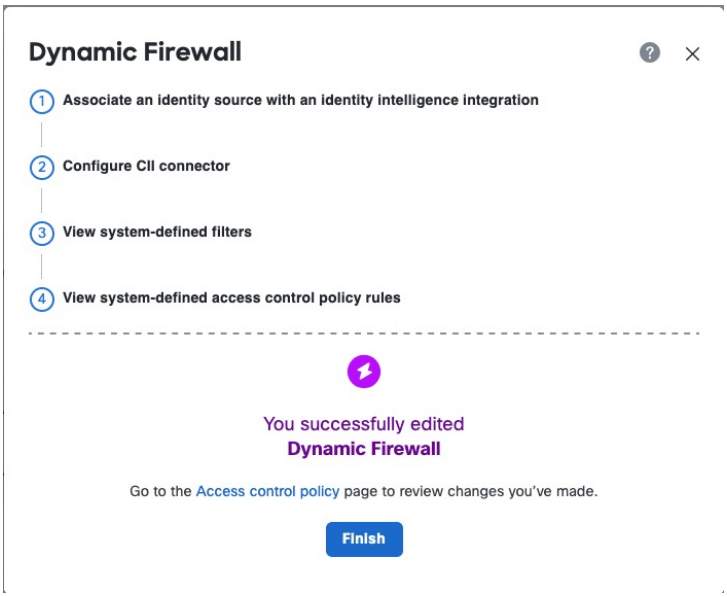
次の図は例を示しています。



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。 （8 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

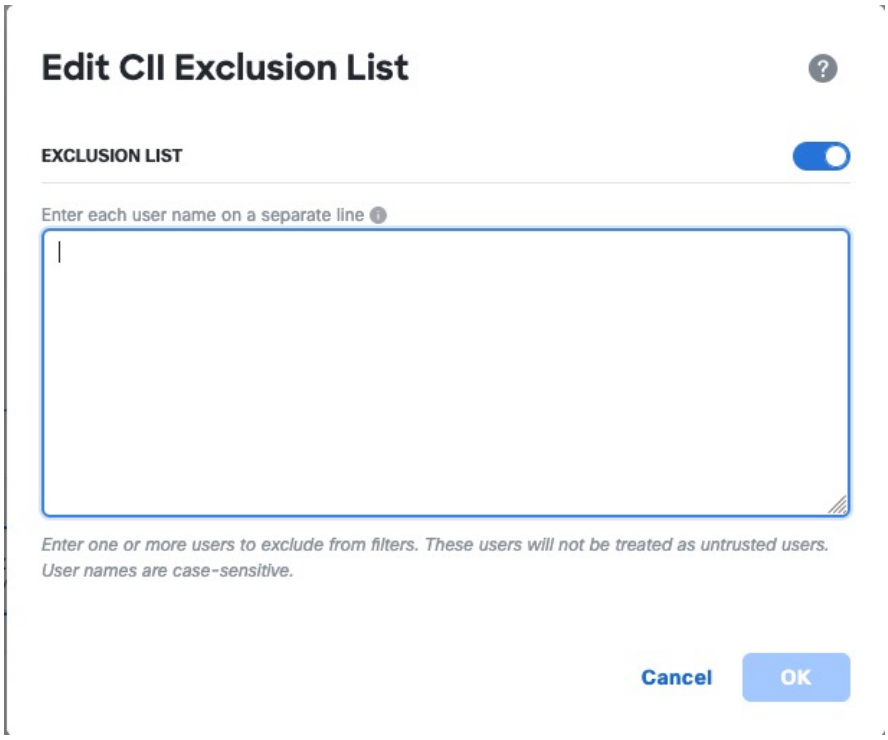
ステップ 1 まだ Cisco Secure Firewall Management Center にログインしていない場合は、ログインします。

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。



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 （13 ページ）」で説明されている操作を完了させます。

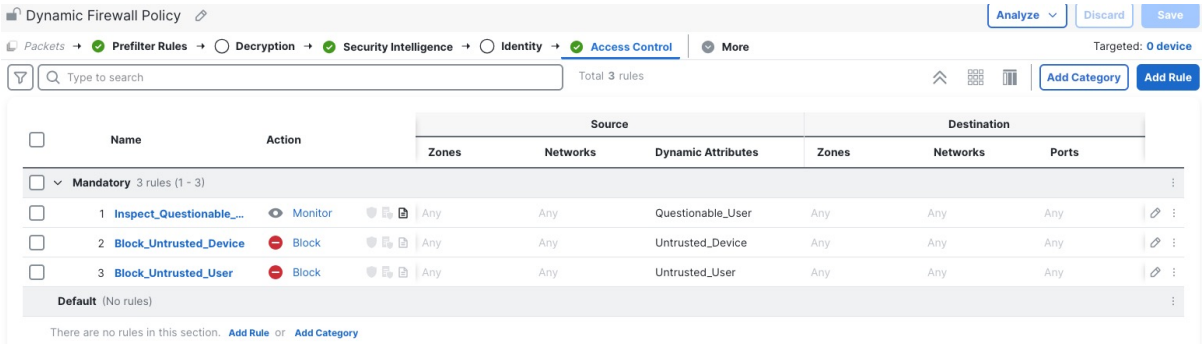
手順

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。



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。 • 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。