アクセス コントロール ルール: レルムとユーザ

次の項では、ネットワークでユーザ トラフィックを制御する方法について説明します。

レルム、ユーザ、ユーザ グループ、および ISE 属性のアクセス コントロール ルール条件

ライセンス: Control

ユーザ制御を実行する（レルム全体、個々のユーザ、ユーザ グループ、または ISE 属性に基づいてアクセス コントロール ルール条件を作成する）前に、次のことを行う必要があります。

- モニタ対象の Microsoft Active Directory または LDAP サーバのそれぞれに対し、レルムを設定する。レルムに対してユーザのダウンロードを有効にすると、FirePOWER Management Center は定期的および自動的に、新規に報告されたかすでに報告済みの権限のあるユーザおよびユーザ グループのメタデータをダウンロードするようサーバに照会します。
- レルムを認証方式に関連付けるために、アイデンティティ ポリシーを作成する。
- 1 つ以上のユーザ エージェントまたは ISE デバイス、あるいはキャプティブ ポータルを設定する。ISE 属性の条件を使用するには、ISE を設定する必要があります。

  ユーザ エージェント、ISE およびキャプティブ ポータルは、アクセス コントロール ルール条件でユーザ制御に使用できる、権限のあるユーザ データを収集します。アイデンティティ ソースは、指定したユーザがホストにログイン、ログアウトしたり、LDAP または AD クレデンシャルを使用して認証する際にモニタします。

（注） ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、FirePOWER Management Center のユーザ制限が原因で、システムがグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルム、ユーザ、またはユーザ グループ条件をもつアクセス コントロール ルールが想定どおりに適用されない可能性があります。

1 つのユーザ条件で、最大 50 のレルム、ユーザおよびグループを [選択されたユーザ（Selected Users）] に追加できます。ユーザ グループを持つ条件は、そのグループのメンバー（サブグループのメンバーを含む）のいずれかが送信元/宛先であるトラフィックを照合します。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

ユーザ グループを含めると、自動的に、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでセカンダリ グループを使用する場合は、明示的にセカンダリ グループを含める必要があります。

(注)　アクセス コントロール ルールがネットワーク トラフィックを評価する前に、ハードウェア ベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、SSL インスペクション、ユーザ識別、および一部のデコードと前処理が行われます。

ユーザ アクセス コントロール ルールに関するトラブルシューティング

ライセンス: Control

ユーザ アクセス コントロール ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。

レルム、ユーザ、またはユーザ グループに対するアクセス コントロール ルールが適用されない

ユーザ エージェントまたは ISE デバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、FirePOWER Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、レルムまたはユーザ条件を使用するアクセス コントロール ルールが想定どおりに適用されない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

ユーザ グループ条件を含むアクセス コントロール ルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、FirePOWER Management Center はユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むアクセス コントロール ルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが FirePOWER Management Center に報告され、ユーザ条件を含むアクセス コントロール ルールでの使用に適するようにカスタマイズする必要があります。

アクセス コントロール ルールが、初めて表示されたユーザに一致していない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバから情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するアクセス コントロール ルールによって処理されません。代わりに、ユーザ セッションは、一致する次のアクセス コントロール ルール（またはアクセス コントロール ポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むアクセス コントロール ルールに一致しない。
- ユーザ データ取得に使用されたサーバが Active Directory サーバである場合に、ISE またはユーザ エージェントによって報告されたユーザがアクセス コントロール ルールに一致しない。

これにより、システムがユーザ データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

アクセス コントロール ルールへのレルム、ユーザ、またはユーザ グループ条件の追加

ライセンス: Control

はじめる前に

- ユーザ アイデンティティ ソース（30-1 ページ）の説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- レルムの作成（29-5 ページ）の説明に従って、レルムを設定します。アクセス コントロール ルールでレルム、ユーザ、またはユーザ グループ条件を設定できるようにするには、その前にユーザによるダウンロード（自動またはオンデマンド）が実行される必要があります。

ステップ 1　アクセス コントロール ルール エディタで、[ユーザ（Users）] タブを選択します。

ステップ 2　[使用可能なレルム（Available Realms）] リストで名前または値で検索してレルムを選択します。

ステップ 3　[使用可能なユーザ（Available Users）] リストで名前または値で検索してレルムを選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。

アクセス コントロール ルールへの ISE 属性条件の追加

ライセンス: Control

はじめる前に

- ISE 接続の設定（30-6 ページ）の説明に従って ISE を設定します。

ステップ 1　アクセス コントロール ルール エディタで、[ISE 属性（ISE Attributes）] タブを選択します。

ステップ 2　[使用可能な ISE セッション属性（Available ISE Session Attributes）] リストで名前または値で検索して属性を選択します。

ステップ 3　[使用可能な ISE メタデータ（Available ISE Metadata）] リストで名前または値で検索してメタデータを選択します。

ステップ 4　[ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ヒント　[ロケーションの IP アドレスの追加（Add a Location IP Address）] フィールドを使用して、条件にロケーションの IP 属性を追加することもできます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-12 ページ）を参照してください。