ISE/ISE-PIC によるユーザの制御

次のトピックでは、ISE/ISE-PIC によりユーザ認識とユーザ制御を実行する方法について説明します。

ISE/ISE-PIC アイデンティティ ソース

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を Firepower システムと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、またはRSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） FirePOWER システムは、マシンの認証をユーザと関連付けないため、Active Directory 認証と同時に 802.1x マシン認証をサポートすることはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン（マシンとユーザの両方）だけを報告するように ISE を設定します。このように設定すれば、マシン ログインはシステムに 1 回だけ報告されます。

Cisco ISE/ISE-PIC の詳細については、*Cisco Identity Services Engine Administrator Guide* および『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*』を参照してください。

ISE/ISE-PIC のガイドラインと制限事項

Firepower システムで ISE/ISE-PIC を構成する際に、このセクションで説明されているガイドラインを使用してください。

ISE/ISE-PIC バージョンと設定の互換性

ご使用の ISE/ISE-PIC バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE/ISE-PIC サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- ISE または ISE-PIC データを使用してユーザ制御を実装するには、レルムの作成の説明に従って、pxGrid のペルソナを想定して ISE サーバのレルムを設定し有効にします。
- 多数のユーザ グループをモニタするように ISE/ISE-PIC を設定した場合、システムはメモリ制限のために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、レルムまたはユーザ条件を使用するルールが想定どおりに実行されない可能性があります。
- ISE のバージョン 2.0 パッチ 4 以降には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE の展開で ISE Endpoint Protection Service（EPS）が有効で設定されている場合は、ISE 接続を使用して、相関ポリシー違反に関与している送信元または宛先ホストに対する ISE EPS 修復を実行できます。
- ユーザの EPSStatus が変更された後でユーザの SGT を更新するように ISE の展開を設定した場合は、ISE EPS 修復により、Firepower Management Center 上の SGT も更新されます。
- ISE-PIC は、ISE 属性データを提供しないか、または ISE EPS の修復をサポートしません。

システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ISE でのクライアントの認証

ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

（注） ISE SGT 属性タグのみを使用してユーザ制御を実装する場合、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。詳細については、ISE 属性条件の設定を参照してください。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。カスタム SGT 条件 を参照してください。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

[エンドポイント ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。これは、ISE-PIC ではサポートされません。

ユーザ制御用 ISE/ISE-PIC の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- レルムの作成の説明に従い、pxGrid ペルソナを想定して ISE サーバのレルムを設定し、有効にします。
- ISE または ISE-PIC への接続を設定します。詳細については、ISE/ISE-PIC アイデンティティ ソース （1 ページ）およびISE/ISE-PIC 設定フィールド （5 ページ）を参照してください。
- 暗号化接続を使用して ISE/ISE-PIC サーバで Firepower Management Center を認証するには、Firepower Management Center のアクセス元となるマシンで証明書データとキーを利用可能にするか、証明書を作成します。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 4 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 5 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 6 [pxGrid サーバ CA（pxGrid Server CA）] および [MNT サーバ CA（MNT Server CA）] リストから該当する認証局を、[FMC サーバ証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、追加アイコン（  ）をクリックして証明書を追加することもできます。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 7 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 8 接続をテストするには、[テスト（Test）] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ（Additional Logs）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用の説明に従って、ユーザ アクティビティをモニタします。

関連トピック

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング （6 ページ）
信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE/ISE-PIC 設定フィールド

次のフィールドを使用して ISE または ISE-PIC への接続を設定します。

プライマリおよびセカンダリ ホスト名/IP アドレス（Primary and Secondary Host Name/IP Address）

プライマリ（およびオプションでセカンダリ）pxGrid ISE サーバのホスト名または IP アドレス。

指定するホスト名により使用されるポートには、ISE と Firepower Management Center の両方から到達可能である必要があります。

pxGrid サーバ CA（pxGrid Server CA）

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバ CA（MNT Server CA）

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

FMC サーバ証明書（FMC Server Certificate）

ISE への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE に提供する必要がある証明書およびキー。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- **任意（Any）**のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの FirePOWER システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

関連トピック

信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシューティングおよびユーザ制御のトラブルシューティングを参照してください。

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE と FirePOWER システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

- [FMC サーバ証明書（FMC Server Certificate）] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードが含まれている場合は、
  - 両方のノードの証明書が、同じ認証局によって署名される必要があります。
  - ホスト名により使用されるポートが、ISE サーバと Firepower Management Center の両方により到達可能である必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE または ISE-PIC によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで**処理されず**、Web インターフェイスに**表示されません**。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザ データを受信できません。
- ISE が TS エージェントと同じユーザをモニタした場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントと ISE が同じ IP アドレスによる同一のアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。
- 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （1 ページ）を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。
- ISE-PIC は ISE EPS の修復を実行できません。

サポートされている機能に問題がある場合は、ISE/ISE-PIC アイデンティティ ソース （1 ページ）で詳細を参照してバージョンの互換性を確認してください。

ISE/ISE-PIC の履歴

機能	バージョン（Version）	詳細（Details）
ISE-PIC との統合	6.2.1	ISE-PIC のデータを使用できるようになりました。
ユーザ制御用の SGT タグ。	6.2.0	ISE セキュリティ グループ タグ（SGT）データに基づいてユーザ制御を実行するために、レルムまたはアイデンティティ ポリシーを作成する必要がなくなりました。
ISE との統合。	6.0	導入された機能。シスコの Platform Exchange Grid（PxGrid）に登録することで、Firepower Management Center で追加のユーザ データ、デバイス タイプデータ、デバイス ロケーションデータ、およびセキュリティ グループ タグ（SGT：ネットワーク アクセス コントロールを提供するために ISE によって使用される方式）をダウンロードできます。