ユーザ アイデンティティ ソース

ASA FirePOWER モジュールは、次のアイデンティティ ソースをサポートしています。

- 権限のあるユーザ エージェント レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ホストにログインまたはホストからログアウトするとき、または Active Directory クレデンシャルで認証するときにユーザをモニタするようにユーザ エージェントを設定するには、ユーザ エージェントのアイデンティティ ソース （4 ページ）を参照してください。
- 権限のあるレポートは、Identity Services Engine（ISE）または ISE-PIC レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ISE/ISE-PIC が展開されていて、Active Directory ドメイン コントローラ（DC）を使用した認証時にユーザをモニタするように ISE/ISE-PIC を設定する場合は、ISE/ISE-PIC アイデンティティ ソース （5 ページ）を参照してください。
- 権限のあるキャプティブ ポータル認証は、アクティブにネットワークのユーザを認証し、ユーザ認識とユーザ制御に関するユーザ データを収集します。キャプティブ ポータル認証を実行するために仮想ルータまたは FirePOWER Threat Defense デバイスを設定する場合は、キャプティブ ポータル アクティブ認証のアイデンティティ ソース （8 ページ）を参照してください。

これらのアイデンティティ ソースからのデータは、ASA FirePOWER モジュール ユーザ データベースおよびユーザ アクティビティ データベースに保存されます。データベース サーバ クエリを設定すると、モジュールに新しいデータを自動的にダウンロードできます。

ASA FirePOWER モジュールでのユーザ検出の詳細については、ユーザ検出の基本を参照してください。

ユーザアイデンティティソースに関する問題のトラブルシューティング

ライセンス：任意

ユーザ アイデンティティ ソースに関する問題のトラブルシューティングについては、次の各項を参照してください。

ユーザ エージェント

ユーザ エージェントの接続に関する問題が発生した場合は、*Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ユーザ エージェント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ユーザ エージェント 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。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が成功するまで、ユーザ エージェント ユーザから見えるアクティビティはアクセス コントロール ルールで処理され、Web インターフェイスに表示されません。

ISE/ISE-PIC

ISE/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。
- すべての ISE システム証明書と FirePOWER Management Center 証明書には、**serverAuth** と **clientAuth** 拡張キー使用値が含まれている必要があります。
- ISE デバイスの時間は、FirePOWER Management Center の時間と同期され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。
- 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/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。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が

成功するまで、ISEユーザから見えるアクティビティはアクセス コントロール ルールで処理され、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。
- ASA FirePOWER モジュールは、ISE ゲスト サービス ユーザのユーザ データは受信しません。
- 使用する ISE バージョンと設定は、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 （5 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。

キャプティブ ポータル

キャプティブ ポータル認証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。

- キャプティブ ポータル サーバの時刻は、ASA FirePOWER モジュールの時刻と同期している必要があります。
- 設定済みの DNS 解決があり、Kerberos（または Kerberos をオプションとする場合は HTTP ネゴシエート）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、キャプティブ ポータルデバイスの完全修飾ドメイン名（FQDN）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- Kerberos（または Kerberos をオプションとする場合は HTTP ネゴシエート）をアイデンティティ ルールの [認証タイプ（Authentication Type）] として選択する場合は、選択する [レルム（Realm）] には、Kerberos キャプティブ ポータル アクティブ認証を実行できるようにするため、[AD 参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] が設定されている必要があります。
- アイデンティティ ルールの [認証タイプ（Authentication Type）] として [HTTP 基本（HTTP Basic）] を選択した場合、ネットワーク上のユーザはセッションがタイムアウトしたことを認識しない場合があります。ほとんどの Web ブラウザは、HTTP 基本ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッドインターフェイスの両方が含まれる場合、キャプティブ ポータルデバイス上でルーテッドインターフェイスだけを対象とするようにキャプティブ ポータルアイデンティティ ルールでゾーン条件を設定する必要があります。

ユーザ エージェントのアイデンティティ ソース

ライセンス：任意

ユーザ エージェントはパッシブ認証方式で、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。ASA FirePOWER モジュールと統合すると、エージェントは、ホストにログインまたはホストからログアウトするとき、あるいは Active Directory クレデンシャルで認証するときにユーザをモニタします。ユーザ エージェントは失敗したログイン試行を報告しません。ユーザエージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

ユーザ エージェントをインストールして使用することで、ユーザ制御を実行できます。つまり、エージェントがユーザと IP アドレスを関連付け、これによりユーザの条件によるアクセス コントロール ルールをトリガーできるようになります。1つのエージェントを使用して最大 5 つの Active Directory サーバ上のユーザ活動を監視できます。

ユーザ エージェントは段階的な設定が必要であり、以下が含まれます。

- エージェントがインストールされたコンピュータまたはサーバ。
- ASA FirePOWER モジュールおよびエージェントがインストールされたコンピュータまたは Active Directory サーバ間の接続。
- ASA FirePOWER モジュールおよびアイデンティティ レルム内のディレクトリとして設定されたモニタ対象 LDAP サーバ間の接続。

段階的なユーザ エージェントの設定とサーバ要件の詳細については、ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ASA FirePOWER モジュール接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。エージェントが特定のユーザ名を除外するように設定されている場合、該当ユーザ名のログイン データは ASA FirePOWER モジュールに報告されません。ユーザ エージェント データは、デバイスのユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を ASA FirePOWER モジュールに送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモートセッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを回避する方法については、ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ユーザ エージェント接続の設定

ライセンス：Control

はじめる前に

ユーザ アクセス コントロールを実装する場合は、レルムの作成の説明に従って、ユーザ エージェント接続用の Active Directory レルムを設定して有効にします。

ユーザ エージェント接続の設定方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration]> [Identity Sources] の順に選択します。 > >

ステップ 2 [Service Type] に [User Agent] を選択し、ユーザ エージェント接続を有効にします。

（注） 接続を無効にするには、[None] を選択します。

ステップ 3 [Add New Agent] ボタンをクリックして、新しいエージェントを追加します。

ステップ 4 エージェントをインストールするコンピュータの [Hostname] または [Address] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように ASA FirePOWER モジュールを設定することはできません。

ステップ 5 [Add] をクリックします。

ステップ 6 接続を削除するには、削除アイコンをクリックして、削除を確認します。

次のタスク

- *Firepower* ユーザ エージェント コンフィギュレーション ガイドの説明に従い、ユーザ エージェントの設定を続行します。

ISE/ISE-PIC アイデンティティ ソース

ライセンス：任意

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を ASA FirePOWER モジュールと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

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 によっ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、AD 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） システムではマシンの認証とユーザが関連付けられないため、ASA FirePOWER モジュールは、AD 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* 管理者ガイドおよび *Identity Services Engine Passive Identity Connector*（*ISE-PIC*）のインストールおよび管理者ガイドを参照してください。

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

- ISE/ISE-PIC サーバと ASA FirePOWER モジュールの時刻を同期させます。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。
- 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。
- ISE のバージョン 2.0 パッチ 4 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-PIC は ISE 属性のデータを提供しません。

このバージョンの ASA FirePOWER モジュール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* 互換性ガイドを参照してください。

ISE 接続を設定すると、ISE 属性データが ASA FirePOWER モジュール 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。

セキュリティ グループ タグ（SGT）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内におけるトラフィックの送信元の権限を指定します。ユーザが TrustSec または ISE でセキュリティ グループを追加すると、セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）が自動的に SGT を生成します。SGA は、パケットがネットワークに入ると、SGT 属性を適用します。ISE をアイデンティティ ソースとして設定するかまたはカスタム SGT オブジェクトを作成することで、アクセス コントロール用に SGT を使用できます。詳細については、ISE SGT およびカスタム SGT ルール条件を参照してください。

SGT ISE 属性ルール条件は、ポリシー内で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設定できます。

エンドポイント ロケーション（ロケーション IP とも呼ばれる）

[Endpoint Location] 属性は Cisco ISE によって適用され、エンドポイント デバイスの IP アドレスを特定します。

関連付けられたアイデンティティ ポリシーがあるポリシー内では、ロケーション IP を ISE 属性ルール条件としてのみ設定できます。

エンドポイント プロファイル（デバイス タイプとも呼ばれる）

[Endpoint Profile] 属性は Cisco ISE によって適用され、各パケットのエンドポイント デバイス タイプを特定します。

関連付けられたアイデンティティ ポリシーがあるポリシー内では、デバイス タイプを ISE 属性ルール条件としてのみ設定できます。

ISE/ISE-PIC フィールド

次のフィールドを使用して ISE/ISE-PIC への接続を設定します。

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）ISE サーバのホスト名または IP アドレス。

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 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。

MC Server Certificate

ISE への接続時、または一括ダウンロードの実行時に ASA FirePOWER モジュールが ISE に提供する必要がある証明書およびキー。

MC サーバ証明書には、**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 Network Filter

ISE がモニタするネットワークを制限するために設定できるオプション フィルタ。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をモニタします。次の方法でフィルタを指定できます。

- すべて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。

ISE/ISE-PIC 接続の設定

ライセンス：Control

はじめる前に

- レルムの作成の説明に従って、レルムを設定します。アクセス コントロール ルールでISE 属性条件を設定するには、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。

（注） SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、またはエンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

ISE/ISE-PIC 接続を設定するには

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration]> [Identity Sources] の順に選択します。 > > >

ステップ 2 [サービス タイプ（Service Type）] に [Identity Services Engine] を選択し、ISE/ISE-PIC 接続を有効にします。

（注） 接続を無効にするには、[None] を選択します。

ステップ 3 [Primary Host Name/IP Address] と、オプションで [Secondary Host Name/IP Address] を入力します。

ステップ 4 [pxGrid Server CA]、[MNT Server CA]、および [MC Server Certificate] ドロップダウンリストから適切な証明書を選択します。必要に応じて、追加アイコンをクリックして、オブジェクトをその場で作成します。

ステップ 5 オプションで、CIDR ブロック表記を使用して **ISE ネットワーク フィルタ** を入力します。

ステップ 6 接続をテストする場合は、[Test] をクリックします。

キャプティブ ポータル アクティブ認証のアイデンティティ ソース

ライセンス：任意

キャプティブ ポータルは、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。これは ASA FirePOWER モジュールでサポートされる唯一のアクティブな認証方式であり、ユーザはデバイスを介してネットワークに対する認証を行うことができます。

キャプティブ ポータル経由のアクティブ認証は、HTTP および HTTPS トラフィックのみで実行されます。HTTPS トラフィックでキャプティブ ポータルを実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号するための、SSL ルールを作成する必要があります。

設定して展開すると、指定レルムのユーザはバージョン 9.5(2) 以降を実行しているルーテッド モードの ASA FirePOWER デバイス経由で認証されます。キャプティブ ポータルから取得された認証データは、ユーザ認識とユーザ制御に使用できます。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行によって新しいユーザがデータベース内のユーザのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザ アクティビティ タイプは、[Failed Auth User] です。

ASA ファイアウォール コンフィギュレーション ガイドの説明に従い、captive-portal ASA CLI コマンドを使用してアクティブ認証のキャプティブ ポータルを有効にします。

アイデンティティ ポリシーのキャプティブ ポータルの設定を続け、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーは、アクセス コントロール ポリシーで呼び出されます。詳細については、キャプティブ ポータル（アクティブ認証）の設定を参照してください。

キャプティブ ポータルは、設定された 1 つ以上のルーテッド インターフェイスがあるデバイスによってのみ実行できます。

アクセス コントロール ルールおよび SSL ルールの次の要件に注意してください。

- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータルに使用する IP アドレスおよびポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定する必要があります。宛先ポートがアクセス コントロール ポリシーで許可されない場合、トラフィックはキャプティブ ポータルを使用して認証できません。

ASA FirePOWER モジュール サーバのダウンロード

ライセンス：任意

ASA FirePOWER モジュールと LDAP または AD サーバ間の接続により、特定の検出されたユーザの、ユーザおよびユーザ グループのメタデータを取得できます。

- キャプティブ ポータルで認証されたか、あるいはユーザ エージェントまたは ISE/ISE-PIC で報告された LDAP および AD のユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出により検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

ASA FirePOWER モジュール ユーザ データベース サーバ接続は、レルム内のディレクトリとして設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[Download users and user groups for access control] チェックボックスをオンにする必要があります。

ASA FirePOWER モジュールは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部門
- 電話番号