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（33-3 ページ）を参照してください。
- 権限のある *Identity Services Engine（ISE）*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 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 を設定する場合は、Identity Services Engine（ISE）のアイデンティティ ソース（33-4 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（33-7 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 クエリーを設定すると、モジュールに新しいデータを自動的にダウンロードすることができます。

ASA FirePOWER モジュールでのユーザ検出の詳細については、ユーザ検出の基礎（31-2 ページ）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（Any）

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 User Agent Configuration Guide*』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 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 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 ユーザに対しては、ユーザ制御を実行できません。
- 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。
- ISE の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、Identity Services Engine（ISE）のアイデンティティ ソース（33-4 ページ）を参照してください。

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、DNS サーバを、キャプティブ ポータル デバイスのホスト名を解決するように設定する必要があります。キャプティブ ポータルのために使用するデバイスのホスト名は、DNS の設定時に入力したホスト名と一致している必要があります。
- 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。

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（Any）

ユーザ エージェントはパッシブな認証方法であり、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、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 サーバでユーザ アクティビティをモニタできます。

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 モジュールと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 サーバとの間の接続。
- ASA FirePOWER モジュールとアイデンティティ 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 サーバとの間の接続。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*User Agent Configuration Guide*』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は、そのような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。これを防ぐ方法については、『*User Agent Configuration Guide*』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（32-5 ページ）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：

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] の順に選択します。

手順 2　[サービス タイプ（Service Type）] に [ユーザ エージェント（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、[なし（None）] を選択します。

手順 3　[新規エージェントの追加（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。

手順 4　エージェントをインストールするコンピュータの [ホスト名（Hostname）] または [アドレス（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。

手順 5　[追加（Add）] をクリックします。

手順 6　接続を削除するには、削除アイコン（ ）をクリックして、その削除を確認します。

次の作業

- 『*FirePOWER User Agent Configuration Guide*』で説明されているユーザ エージェントの設定を続行します。

Identity Services Engine（ISE）のアイデンティティ ソース

ライセンス：任意（Any）

Cisco Identity Services Engine（ISE）内の pxGrid アイデンティティ マッピング機能はパッシブな認証方法であり、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、この ISE 機能によって、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します。LDAP、RADIUS、または RSA ドメイン コントローラで認証されたユーザに対しては、ユーザ制御を実行できません。

ISE は、ログイン試行の失敗や ISE ゲスト サービス ユーザのアクティビティについては報告しません。

ISE から取得されたデータは、ASA FirePOWER モジュールで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。

（注）　ASA FirePOWER モジュールは、Active Directory 認証と並行して 802.1x マシン認証をサポートしていません。現在のところ、システムはユーザとマシン認証を関連付ける方法がないためです。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 を設定する必要があります。この提案された構成では、マシン ログインは ASA FirePOWER モジュールに一度だけ報告されます。後続のマシン ログインは報告されません。

FirePOWER システムのこのバージョンは、Cisco ISE のバージョン 1.3 およびバージョン 2.0 をサポートします。ISE の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。たとえば、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 のバージョン 1.3 を実行している場合、ユーザ アイデンティティ データを収集したり、IPv6 対応エンドポイント上で修正を実行したりすることはできません。

注意　多数のユーザ グループをモニタするように ISE を設定する場合、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。

（注）　ISE デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。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。

また、ISE 接続を設定すると、ASA FirePOWER モジュールのデータベースに ISE 属性データとして、[セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]、[エンドポイント プロファイル（Endpoint Profile）]、および [エンドポイント ロケーション（Endpoint Location）] が入力されます。ISE 属性は、ユーザ認識とアクセス コントロール ルールの条件に使用できます。

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。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）により、SGT が自動的に生成されます。パケットがネットワークに入ると、SGA によって SGT 属性が適用されます。SGT をアクセス コントロールに使用するには、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します。詳細については、ISE SGT ルール条件とカスタム SGT ルール条件との比較（10-1 ページ）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）

[エンドポイント ロケーション（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）

[エンドポイント プロファイル（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。

Cisco ISE 製品の詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

ISE フィールド

次のフィールドを使用して ISE 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）ISE サーバのホスト名または IP アドレス。

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。

MC サーバ証明書（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（MC 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）

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 接続の設定

ライセンス：Control

はじめる前に

- レルムの作成（32-5 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 ISE 属性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。

（注）　SGT ISE 属性条件を設定すること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、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 接続を設定するには、次の手順を実行します。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] の順に選択します。

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

（注）　接続を無効にするには、[なし（None）] を選択します。

手順 3　[プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）] と、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。

手順 4　[pxGrid サーバ CA（pxGrid Server CA）]、[MNT サーバ CA（MNT Server CA）]、および [MC サーバ証明書（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。オプションで、追加アイコン（ ）をクリックしてオブジェクトを即座に作成します。

手順 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。

手順 6　接続をテストする場合は、[テスト（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（Any）

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。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通じてネットワークに認証できます。

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 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。失敗した試行で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 [認証失敗ユーザ（Failed Auth User）] です。

`captive-portal` ASA CLI コマンドを使用して、使用バージョンの『*ASA Firewall Configuration Guide*』の説明に従ってキャプティブ ポータルのアクティブ認証を有効にします（http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html [英語]）。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（32-10 ページ）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 インターフェイスを使用してデバイスによってのみ実行できます。

システムは ASA with FirePOWER デバイスでインターフェイス タイプを検証しません。ASA with FirePOWER デバイス上でインライン（タップ モード）インターフェイスにキャプティブ ポータル ポリシーを適用すると、ポリシーは正常に展開されますが、これらのルールに一致するトラフィック内のユーザは「不明」と識別されます。

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。

- 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。
- 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。

ASA FirePOWER モジュール サーバのダウンロード

ライセンス: 任意（Any）

ASA FirePOWER モジュールと LDAP または AD サーバ間の接続により、次の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することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD 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 ベースの検出で検出された 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、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード（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
- 部署
- 電話番号