アイデンティティ データの概要

アイデンティティ ポリシーは、ユーザ エージェント、ISE/ISE-PIC デバイス、またはキャプティブ ポータルを使用して、ネットワーク上のユーザに関するデータを取得するように設定できます。詳細については、ユーザ アイデンティティ ソース を参照してください。

アイデンティティ データの用途

アイデンティティ データを収集することにより、以下を含む多くの機能を活用できます。

- レルム、ユーザ、ユーザ グループ、および ISE 属性条件を使用してアクセス コントロール ルールを作成することにより、ユーザ制御を実行します。
- 特定のインパクト フラグが設定された侵入イベントをシステムが生成すると、電子メール、SNMP トラップ、または syslog により警告が出されます。

ユーザ検出の基本

アイデンティティ ポリシーを使用してネットワーク上のユーザ活動をモニタできます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポートスキャンを開始した人物
- ホスト重要度の高いサーバの不正アクセスを試みている人物
- 不合理な容量の帯域幅を使用している人物

- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を利用して ASA FirePOWER モジュールの他の機能を使用すると、リスクを軽減し、アクセス コントロールを実行し、その他の機能を中断から保護するアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザ アイデンティティ ソースを設定したら、ユーザ対応とユーザ制御を実行できます。

ユーザ対応

ユーザ データの表示や分析ができます。

ユーザ制御

ユーザ アクセス コントロール ルール条件を設定して、ユーザ対応から引き出した結論に基づいて、ネットワーク上のトラフィックでユーザやユーザ アクティビティをブロックできます。

ユーザ データは、正規のアイデンティティ ソース（アイデンティティ ポリシーにより参照される）から取得できます。

アイデンティティ ソースは、信頼できるサーバによりユーザ ログインが検証済みであれば、正規のものになります。正規のログインから取得されるデータを使用して、ユーザ対応とユーザ制御を実行できます。正規のユーザ ログインは、パッシブ認証とアクティブ認証から取得されます。

- パッシブ認証は、ユーザが外部サーバで認証するときに実行されます。ASA FirePOWER モジュールでサポートされているパッシブ認証方式は、ユーザ エージェントと ISE/ISE-PIC だけです。
- アクティブ認証は、ユーザが FirePOWER デバイスにより認証するときに実行されます。ASA FirePOWER モジュールでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

次の表に、ASA FirePOWER モジュールでサポートされているユーザ アイデンティティ ソースの概要を示します。

ユーザ アイデンティティ ソース	サーバ要件	ソース タイプ	認証タイプ	ユーザ認識	ユーザ アクセス コントロール	詳細情報の参照先
ユーザ エージェント	Microsoft Active Directory	正規のログイン	パッシブ	対応	対応	ユーザ エージェントのアイデンティティ ソース
ISE/ISE-PIC	Microsoft Active Directory	正規のログイン	パッシブ	対応	対応	ISE/ISE-PIC アイデンティティ ソース

ユーザアイデンティティ ソース	サーバ要件	ソース タイプ	認証タイプ	ユーザ認識	ユーザ アクセス コントロール	詳細情報の参照先
キャプティブ ポータル	LDAP または Microsoft Active Directory	正規のログイン	アクティブ	対応	対応	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

展開するアイデンティティ ソースを選択するには、以下を考慮します。

- キャプティブ ポータルを使用して、失敗した認証アクティビティを記録する必要があります。失敗認証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 ポータルを使用するために、センシング インターフェイス（ルーテッド インターフェイスなど）の IP アドレスがあるアプライアンスを展開する必要があります。

ユーザ アイデンティティの展開

システムが任意のアイデンティティ ソースからのユーザ データをユーザ ログイン時に検出すると、そのログインのユーザは、ユーザ データベース内のユーザのリストに照らして確認されます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザ活動データベース

デバイス上のユーザ アクティビティ データベースには、設定済みのすべてのアイデンティティ ソースにより報告された、ネットワーク上のユーザ アクティビティのレコードが含まれています。システムは次の状況でイベントを記録します。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ制限に達したためにそのユーザを追加できなかったとき

ユーザ データベース

ユーザ データベースには、設定済みのアイデンティティ ソースにより報告された、各ユーザのレコードが含まれています。

デバイスが保存できるユーザの合計数は、モデルごとに異なります。制限に達した場合は、ユーザを（手動またはデータベースの消去により）削除して、新規ユーザを追加できるようにする必要があります。

アイデンティティ ソース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、それらのユーザ名のユーザ アクティビティ データは ASA FirePOWER モジュールに報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

現在のユーザ アイデンティティ

異なる複数のユーザによる同じホストへの複数のログインがシステムにより検出されると、特定のホストに同時にログインできるのは1ユーザのみであり、ホストの現在のユーザが最新の正式なユーザ ログインであると見なされます。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが ASA FirePOWER モジュールに報告されるユーザです。

同じユーザによる同じホストへの複数のログインがシステムにより検出されると、システムは指定のホストへのユーザの最初のログインを記録し、それ以降のログインは無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

ユーザ データベースの制限

デバイス モデルにより、モニタできるユーザの数、およびユーザ制御を実行するために使用できるユーザ数が決定されます。

ASDM によって管理される ASA FirePOWER モジュールを展開する場合、最大 2,000 の正規ユーザをユーザ データベースに保存できます。