ネットワーク検出とアイデンティティの概要

次のトピックでは、ネットワーク検出およびアイデンティティ ポリシーとデータの概要を示します。

ホスト、アプリケーション、およびユーザのデータの検出について

Firepower システムは、ネットワーク検出およびアイデンティティ ポリシーを使用して、ネットワーク トラフィックのホスト、アプリケーション、およびユーザのデータを収集します。特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーション データ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティ ソースとアプリケーション ディテクタによって収集されます。管理対象デバイスは、指定したネットワーク セグメントのトラフィックを確認します。

詳細については、ホストおよびアプリケーション検出の基礎 （3 ページ）を参照してください。

ユーザ データ（User Data）

ユーザ データはネットワーク検出およびアイデンティティ ポリシーの設定に従ってユーザのアイデンティティ ソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、ユーザ アイデンティティについて （11 ページ）を参照してください。

検出データとアイデンティティ データをロギングすることにより、次のような Firepower システムのさまざまな機能を活用できます。

- ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示できます。
- アプリケーション、レルム、ユーザ、ユーザ グループ、およびISE属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルを表示します。
- （さまざまな機能の 1 つとして）ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
- システムによって記録された検出イベントとユーザアクティビティに関する詳細情報を表示します。
- ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。

  これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワーク アセットを最大限に保護できるように侵入ルール状態を調整したりできます。
- システムで特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントが生成された場合に、電子メール、SNMP トラップ、または syslog によるアラートを発行します。
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイトリストを使用して組織のコンプライアンスをモニタします。
- システムが検出イベントを生成するかユーザアクティビティを検出したときにトリガーして相関イベントを生成するルールを使って、相関ポリシーを作成します。
- 該当する場合、NetFlow 接続をロギングして使用します。

関連トピック

ホスト ID ソース
アプリケーションの検出
ユーザ アイデンティティ ソース

ホスト、アプリケーション、ユーザの検出

Firepower システムは、ネットワーク検出およびアイデンティティ ポリシーを使用して、ネットワーク トラフィックのホスト、アプリケーション、およびユーザのデータを収集します。特定のタイプの検出およびアイデンティティ データを使用すると、ネットワーク アセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーション データ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティ ソースとアプリケーション ディテクタによって収集されます。管理対象デバイスは、指定したネットワーク セグメントのトラフィックを確認します。

詳細については、ホストおよびアプリケーション検出の基礎 （3 ページ）を参照してください。

ユーザ データ（User Data）

ユーザ データはネットワーク検出およびアイデンティティ ポリシーの設定に従ってユーザのアイデンティティ ソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、ユーザ アイデンティティについて （11 ページ）を参照してください。

関連トピック

ホスト ID ソース
アプリケーションの検出
ユーザ アイデンティティ ソース

ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、概要：ホストのデータ収集および概要：アプリケーション検出を参照してください。

オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出は、システムがネットワーク トラフィック（およびエクスポートされたNetFlowデータ）を分析してネットワーク マップにデータを取り込む際のデフォルト方式です。パッシブ検出では、ネットワーク アセットに関するコンテキスト情報（オペレーティング システムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトラフィックが、ホストで実行されているオペレーティング システムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングが

ネットワーク マップに表示されます。たとえば、複数のホストが NAT デバイスの「背後」にあることから、NAT デバイスが複数のオペレーティング システムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのは、検出された各オペレーティング システムに割り当てられた信頼度の値と、検出されたオペレーティング システムの中でその特定のオペレーティング システムが使用されていることを裏付けるデータの量です。

（注） この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティング システムを考慮しません。

パッシブ検出でネットワーク アセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティング システムのカスタム フィンガープリントとカスタム アプリケーション ディテクタで増補することもできます。あるいは、アクティブ検出を使用するという方法もあります。アクティブ検出では、トラフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワーク マップを更新できます。

オペレーティング システムおよびホスト データのアクティブ検出

アクティブ検出では、アクティブ ソースによって収集されたホスト情報をネットワーク マップに追加します。たとえば、Nmap スキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmap は、ホストでオペレーティング システムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワーク マップにホスト入力データをアクティブに追加することができます。ホスト入力データには 2 種類のカテゴリがあります。

- ユーザ入力データ：FirePOWER システム ユーザ インターフェイスで追加されたデータ。このユーザ インターフェイスを使用して、ホストのオペレーティング システムやアプリケーションの ID を変更できます。
- ホスト インポート入力データ：コマンド ライン ユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブ ソースに対して 1 個の ID を保持します。たとえば、Nmap スキャンインスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmap スキャンを実行し、それらの結果をクライアントからのデータ（コマンド ラインを使用してインポートした結果）と交換する場合、システムは Nmap の結果の ID とインポート クライアントの ID の両方を保持します。システムは、ネットワーク検出ポリシーで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザが入力したとしても、ユーザ入力は 1 ソースと見なされることに注意してください。たとえば、UserA がホスト プロファイルを使用してオペレーティング システムを設定し、UserB がホスト プロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザ入力によっ

て、他のアクティブ ソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

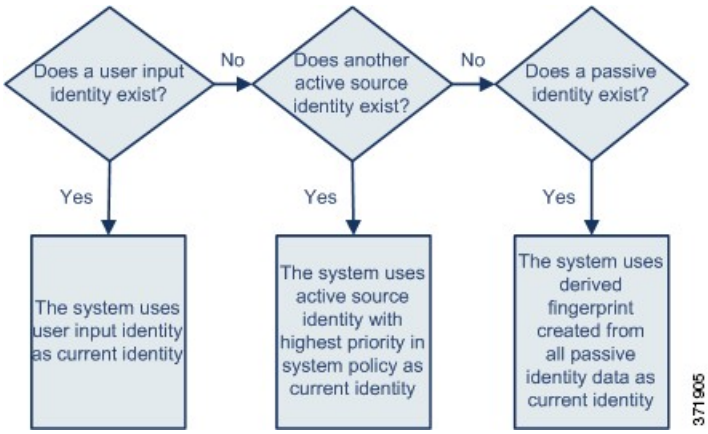
アプリケーションおよびオペレーティング システムの現在の ID

ホストのアプリケーションまたはオペレーティング システムの現在の *ID* は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティング システムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティング システムの識別、ホスト プロファイルの認定、およびコンプライアンスのホワイトリストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバのテーブル ビューでの表示
- ホスト プロファイルでの表示
- [検出統計情報（Discovery Statistics）]ページでのオペレーティング システムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティング システムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザがホストでオペレーティング システムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱性を狙った攻撃により大きな影響力があると見なされ、ホストプロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含められます。

データベースは、ホストのオペレーティング システムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティング システムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1. ユーザ

2. スキャナとアプリケーション（ネットワーク検出ポリシーで設定）

3. 管理対象デバイス

4：NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

現在のユーザ ID

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。権限のないユーザ ログインだけがホストにログインしている場合は、最後にログインしたものが現在のユーザと見なされます。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 Firepower Management Centerに報告されるユーザです。

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。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。

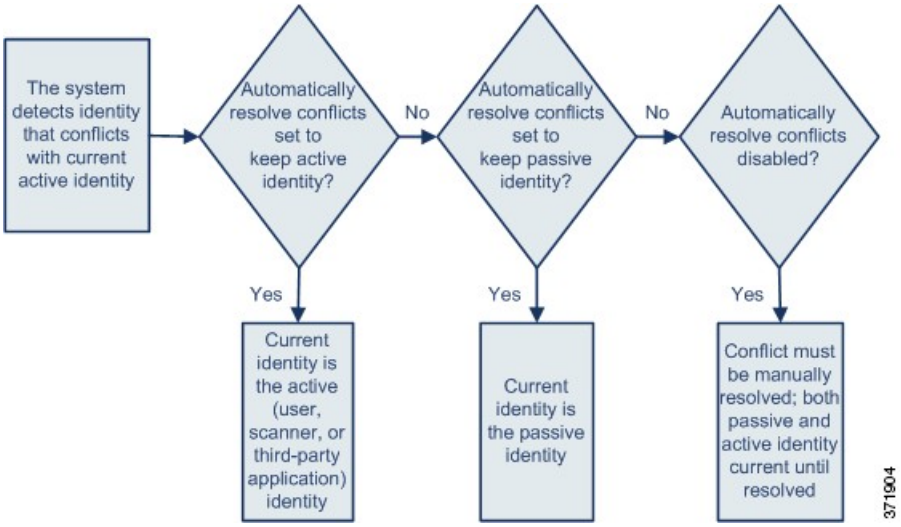
ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

アプリケーションおよびオペレーティング システムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、*ID* の競合が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

ホストのオペレーティング システムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティング システムとアプリケーション データを取得します。

Firepower システムの NetFlow データ

NetFlow は、ルータを通過するパケットの統計情報を提供する、Cisco IOS アプリケーションの 1 つです。NetFlow は Cisco ネットワーキング デバイスで使用できます。また、Juniper、FreeBSD、OpenBSD デバイスに組み込むことも可能です。

NetFlow がネットワーク デバイスで有効にされている場合、そのデバイス上のデータベース（NetFlow キャッシュ）に、ルータを通過するフローのレコードが格納されます。Firepower システムで接続と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーション プロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。この NetFlow データをエクスポートするようにネットワーク デバイスを設定できます。本書では、そのように設定されたネットワーク デバイスを NetFlow エクスポータと呼びます。

Firepower システムの管理対象デバイスは、NetFlow エクスポータからレコードを収集して、それらのレコードに含まれるデータに基づいて単方向の接続終了イベントを生成し、それらのイベントを接続イベント データベースに記録するために Firepower Management Center に送信するように設定できます。また、NetFlow 接続内の情報に基づいて、ホストとアプリケーション プロトコルに関する情報をデータベースに追加するためのネットワーク検出ポリシーを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニタできないネットワークを NetFlow エクスポータにモニタさせる場合には特に有効です。

NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他の NetFlow が有効なネットワーク デバイス上で NetFlow 機能を有効にし、管理対象デバイスのセンシング インターフェイスを接続する宛先ネットワークへ NetFlow データをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower System にデータをエクスポートするには、NetFlow エクスポータがいずれかのバージョンを使用する必要があります。さらに、このシステムでは、特定のフィールドがエクスポートされた NetFlow テンプレートとレコードに存在する必要があります。NetFlow エクスポータがカスタマイズ可能なバージョン 9 を使用している場合は、エクスポートされたテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する必要があります。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System は管理対象デバイスを使用して NetFlow データを分析するため、NetFlow エクスポータの監視可能な 1 つ以上の管理対象デバイスを展開に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、エクスポートされた NetFlow データを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

一部のネットワーク デバイス上で使用可能な Sampled NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、ネットワーク デバイス上の CPU 使用率が改善される可能性がありますが、Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

NetFlow データと管理対象デバイス データの違い

Firepowerシステムは、NetFlowデータによって表されるトラフィックを直接分析しません。代わりに、エクスポートしたNetFlowレコードを接続ログおよびホストとアプリケーションのプロトコル データに変換します。

その結果、変換されたNetFlowデータと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、これらの違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

接続ロギングを含むNetFlowデータ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロール ルールごとに設定したFirePOWERシステム管理対象デバイスによって検出された接続の接続ロギングと比較してください。

接続イベントのタイプ

NetFlowデータ収集はアクセス コントロール ルールではなくネットワークにリンクされているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティ インテリジェンス イベントを生成することはできません。

NetFlowベースの接続イベントは、接続イベント データベースにのみ保存できます。システム ログまたは SNMP トラップ サーバに送信することはできません。

モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルールを設定して、接続の最初か最後またはその両方で双方向接続イベントをログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも 2 つの接続イベントを生成します。これは、概要の接続数がNetFlowデータに基づいた接続ごとに2ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続がまだ実行中であっても、NetFlow エクスポータは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があり、その各レコードが接続イベントを生成します。たとえば、NetFlow エクスポータが 5 分ごとにエクスポートする場合に、特定の接続が12分間続いている場合、システムはそのセッションに対し 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア

- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

ホスト データとオペレーティング システム データ

NetFlowデータからのネットワーク マップに追加されたホストには、オペレーティング システム、NetBIOS、またはホスト タイプ（ホストまたはネットワーク デバイス）の情報がありません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーション プロトコル、クライアント、およびWebアプリケーションを識別できます。

システムはNetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーション プロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーション プロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

システムは、ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID を手動で設定しない限り、NetFlow エクスポータによってモニタされるホストに脆弱性をマッピングできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性をNetFlowデータから作成されたホストに関連付けることはできないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

Firepowerシステムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の小さい方のポートを使用しているホストを応答側と見なします。

- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1～1023の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの2バイト数を記録します。

- [イニシエータ バイト数（Initiator Bytes）] フィールドは送信バイト数を記録します。
- [レスポンダ バイト数（Responder Bytes）] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1バイト数しか含まれておらず、ポートベース アルゴリズムに応じて、システムが [イニシエータ バイト数（Initiator Bytes）] または [レスポンダ バイト数（Responder Bytes）] に割り当てます。システムによって他のフィールドは0に設定されます。NetFlow レコードの接続の概要（集約接続データ）を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます（接続イベント フィールドで利用可能な情報を参照）。

関連トピック

接続イベント フィールドで利用可能な情報

ユーザ アイデンティティについて

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。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。
- 特定のホストへの不正アクセスを試みている人物。
- 過度に大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。
- ネットワーク上の侵害の兆候に関連付けられている人物。

この情報を入手すれば、Firepower システムの他の機能を使用して、リスクを低減し、アクセス制御を実行し、他のユーザを破壊行為から保護するための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 ソースを設定してユーザ データを収集すると、ユーザ認識とユーザ制御を実行できます。

関連トピック

アイデンティティの用語 （12 ページ）
アイデンティティ導入 （15 ページ）
ユーザ アイデンティティ ソースについて （13 ページ）
アイデンティティ ポリシーの設定方法 （15 ページ）

アイデンティティの用語

このトピックでは、ユーザアイデンティティおよびユーザ制御の一般的な用語について説明します。

ユーザ認識

アイデンティティ ソース（ユーザ エージェントや TS エージェントなど）を使用して、ネットワーク上のユーザを識別します。ユーザ認識によって、権限のあるソース（Active Directory など）および権限のないソース（アプリケーションベース）の両方からユーザを識別できます。Active Directory をアイデンティティ ソースとして使用するには、レルムおよびディレクトリを設定する必要があります。詳細については、ユーザアイデンティティ ソースについて （13 ページ）を参照してください。

ユーザ制御

アクセス コントロール ポリシーに関連付けるアイデンティティ ポリシーを構成します。（アイデンティティ ポリシーは、アクセス コントロール サブポリシーと呼ばれるようになります。）アイデンティティ ポリシーはアイデンティティ ソースを指定し、オプションで、そのソースに属するユーザおよびグループを指定します。

アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けることで、ネットワークのトラフィックでユーザまたはユーザアクティビティをモニタ、信頼、ブロックまたは許可するかどうかを決定します。詳細については、アクセス コントロール ポリシーの開始を参照してください。

権限のあるアイデンティティ ソース

信頼できるサーバによってユーザ ログインが検証されています（たとえば、Active Directory）。権限のあるログインから取得したデータを使用すると、ユーザ認識とユーザ制御を実行できます。権限のあるユーザ ログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザが外部ソース経由で認証されるときに発生します。ユーザ エージェント、ISE/ISE-PIC、および TS エージェントは、Firepower システムでサポートされるパッシブ認証方式です。

- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。キャプティブ ポータルおよびリモート アクセス VPN は、Firepower システムでサポートされるアクティブ認証方式です。

権限のないアイデンティティ ソース

ユーザ ログインの検証を行った不明または信頼できないサーバ。トラフィック ベースの検出は、Firepowerシステムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザ認識を実行できます。

ユーザ アイデンティティ ソースについて

次の表に、Firepower システム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。各アイデンティティ ソースは、ユーザ認識のためのユーザの記憶域を提供します。これらのユーザは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ（Type）	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
ユーザ エージェント	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	ユーザ エージェントのアイデンティティ ソース
ISE/ISE-PIC	アイデンティティ	Microsoft Active Directory	権限のあるログイン	パッシブ	○	○	ISE/ISE-PIC アイデンティティ ソース
TS エージェント	アイデンティティ	Microsoft Windows Terminal Server	権限のあるログイン	パッシブ	○	○	ターミナル サービス（TS）エージェントのアイデンティティ ソース
キャプティブ ポータル	アイデンティティ	LDAP または Microsoft Active Directory	権限のあるログイン	Active	○	○	キャプティブ ポータルのアイデンティティ ソース

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ（Type）	認証タイプ（Authentication Type）	ユーザ認識	ユーザ制御	詳細
リモート アクセス VPN	ID（Identity）	RADIUS、LDAP、または Microsoft Active Directory	権限のあるログイン	Active	○	○	リモート アクセス VPN アイデンティティ ソース
トラフィック ベースの検出	ネットワーク検出	適用対象外	権限のないログイン	適用対象外	[はい（Yes）]	[いいえ（No）]	トラフィック ベース検出のアイデンティティ ソース

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザ ログインにはトラフィック ベースの検出を使用する必要があります。たとえば、ユーザ エージェントのみを使用してユーザ アクティビティを検出している場合は、非 LDAP ログインを制限しても効果はありません。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは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 ポータルのアイデンティティ ソースには、ルーテッド インターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

これらのアイデンティティ ソースからのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに格納されます。Firepower Management Center サーバ ユーザ ダウンロードを設定して、新しいユーザ データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

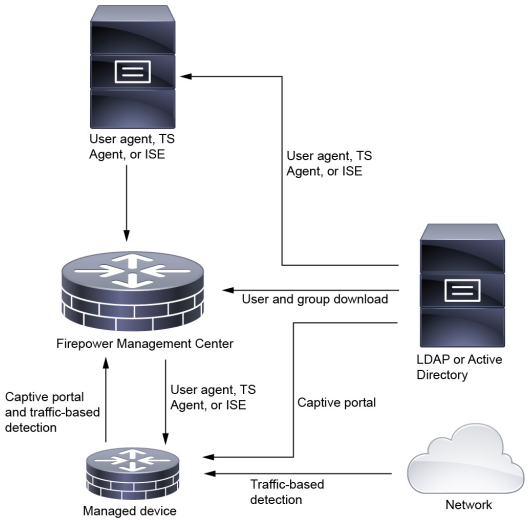
必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセス コントロール ポリシーおよび展開の詳細については、ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）を参照してください。

Firepower システムでのユーザ検出の一般情報については、ユーザ アイデンティティについて（11 ページ）を参照してください。

アイデンティティ導入

システムがユーザ ログイン、またはアイデンティティ ソースからのユーザ データを検出すると、そのログインからのユーザは、Firepower Management Center ユーザ データベース内のユーザのリストに照らしてチェックされます。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。

次の図は、Firepower システムがユーザ データをどのように収集して保存するかを示しています。



アイデンティティ ポリシーの設定方法

このトピックでは、使用可能な任意のユーザ アイデンティティ ソース（TS エージェント、ユーザ エージェント、キャプティブ ポータル、またはリモート アクセス VPN）を使用してアイデンティティ ポリシーを設定する方法の大まかな概要を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	レルムを作成します。	レルムとは、信頼されたユーザおよびグループの領域で、Microsoft Active Directory リポジトリなどがあります。Firepower Management Center は、指定した間隔でユーザとグループをダウンロードします。ユーザやグループをアイデンティティ ポリシーの検討対象に

	コマンドまたはアクション	目的
		含めたり、除外したりできます。レルムの作成を参照してください。
ステップ 2	レルムにディレクトリを作成します。	ディレクトリとは、コンピュータネットワークのユーザとネットワーク共有に関する情報を編成する Active Directory ドメイン コントローラのことです。Active Directory コントローラはレルムにディレクトリ サービスを提供します。Active Directory は、ユーザ オブジェクトやグループ オブジェクトを複数のドメイン コントローラ間に分散させます。これらのドメイン コントローラは、ディレクトリ サービスを使用してローカルの変更を互いに伝達するピアです。詳細については、MSDN の『Active Directory technical specification glossary』[英語] を参照してください。 1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。 レルム ディレクトリの設定を参照してください。
ステップ 3	レルムからユーザやグループをダウンロードします。	ユーザやグループを制御するには、それらを Firepower Management Center にダウンロードする必要があります。ユーザやグループを必要に応じて手動でダウンロードすることも、指定した間隔でシステムがそれらをダウンロードするように設定することもできます。 ユーザやグループをダウンロードするときに、例外を指定できます。たとえば、そのレルムのすべてのユーザ制御から Engineering というグループを除外したり、Engineering グループに適用さ

	コマンドまたはアクション	目的
		れるユーザ制御から **joe.smith** というユーザを除外したりできます。 ユーザとグループのダウンロードを参照してください。
ステップ 4	レルムを有効化します。	ユーザ制御でレルムを使用するには、そのレルムを有効化する必要があります。レルムを有効化するには、[状態（State）] スライダを右にスライドさせます。参照先： レルムの管理 。
ステップ 5	ユーザデータやグループデータを取得するための手法（アイデンティティ ソース）を作成します。	レルムに保存されたデータを使用してユーザやグループを制御するには、固有の設定を使って ID ストアをセットアップします。アイデンティティ ソースには、TS エージェント、ユーザ エージェント、キャプティブ ポータル、またはリモート VPN が含まれます。次のいずれかを参照してください。 • ユーザ制御のためのキャプティブ ポータルの設定方法 • ユーザ制御のためのユーザ エージェントの設定 • ユーザ制御用 ISE/ISE-PIC の設定 • ユーザ制御用 RA VPN の設定
ステップ 6	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーには、1 つ以上のアイデンティティ ルールが含まれており、必要に応じてこれらをカテゴリにまとめることができます。アイデンティティ ポリシーの作成を参照してください。
ステップ 7	1 つ以上のアイデンティティ ルールを作成します。	アイデンティティ ルールを使用すると、認証の種類、ネットワーク ゾーン、ネットワークまたは地理位置情報、レルムなど、多数の一致条件を指定できます。アイデンティティ ルールの作成を参照してください。

	コマンドまたはアクション	目的
ステップ 8	アイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます。	アクセス コントロール ポリシーはトラフィックをフィルタリングし、必要に応じてトラフィックを検査します。アクセス制御への他のポリシーの関連付けを参照してください。
ステップ 9	少なくとも 1 つの管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを使用してユーザアクティビティを制御するには、クライアントの接続先となる管理対象デバイスにそのポリシーを展開する必要があります。設定変更の展開を参照してください。
ステップ 10	ユーザ アクティビティをモニタします。	ユーザアイデンティティ ソースによって収集されたアクティブセッションの一覧、またはユーザアイデンティティ ソースによって収集されたユーザ情報の一覧を確認します。ワークフローの使用を参照してください。

関連トピック

トラフィック ベースのユーザ検出の設定

ユーザ アクティビティ データベース

Firepower Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または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。システムがイベントを記録するのは以下のような状況です。

- 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。
- システム管理者が手動でユーザを削除したとき。
- 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、ユーザ数の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。
- ユーザに関連付けられている侵害の兆候を解決したとき、またはユーザに対して侵害の兆候ルールを有効または無効にしたとき。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントや ISE/ISE-PIC など）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムで検出されたユーザ アクティビティは、Firepower Management Center Web インターフェイスを使用して表示できます。（[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）]）。

ユーザ データベース

Firepower Management Center のユーザ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたユーザごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティ ソースと権限のあるアイデンティティ ソースの詳細については、ユーザ アイデンティティ ソースについて （13 ページ） を参照してください。

Firepower システムのユーザの制限 （21 ページ） で説明されているように、Firepower Management Center で保存できるユーザの合計数は、Firepower Management Center のモデルごとに異なります。ユーザ制限に達した後、システムは、アイデンティティ ソースに基づいて未検出ユーザ データを次のように優先順位付けします。

- 新しいユーザが権限のないアイデンティティ ソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

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 Firepower Management Center 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。システムによって保存されるデータのタイプの詳細については、ユーザ データ（User Data）を参照してください。

Firepower Management Center ハイ アベイラビリティが設定済みで、プライマリに障害が発生した場合、ユーザ エージェント、ISE/ISE-PIC、TS エージェント、リモート アクセス VPN、またはキャプティブ ポータル デバイスから報告されるログインはフェールオーバー ダウンタイム中に識別不能になります（たとえユーザが以前に確認されて Firepower Management Center にダウンロードされた場合でも）。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイムの後に、[不明（Unknown）] のユーザはアイデンティティ ポリシーのルールに従って再度識別されてから処理されます。

（注） TS エージェントが別のパッシブ認証のアイデンティティ ソース（ユーザ エージェントまたは ISE/ISE-PIC）と同じユーザをモニタする場合、Firepower Management Center では TS エージェントのデータを優先します。TS エージェントと別のパッシブのソースが同じ IP アドレスからの同じアクティビティを報告した場合、TS エージェントのデータだけが Firepower Management Center に記録されます。

システムが新しいユーザ セッションを検出すると、そのユーザ セッションのデータは、次のいずれかが発生するまでユーザ データベースに残ります。

- Firepower Management Center のユーザが手動でユーザ セッションを削除した。
- アイデンティティ ソースがそのユーザ セッションのログオフを報告した。
- レルムがレルムの [ユーザ セッションのタイムアウト：認証されたユーザ（User Session Timeout: Authenticated Users）] 設定、[ユーザ セッションのタイムアウト：認証に失敗したユーザ（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザ セッションのタイムアウト：ゲスト ユーザ（User Session Timeout: Guest Users）] 設定で指定されているユーザ セッションを終了した。

Firepower システムのホストとユーザの制限

Firepower Management Center モデルにより、展開でモニタできる個別のホストの数、モニタし、ユーザ制御を実行するために使用できるユーザの数が決定されます。

関連トピック

Management Center データベースからのデータの消去

Firepower システムのホスト制限

システムは（ネットワーク検出ポリシーで定義されている）モニタ対象ネットワークで IP アドレスに関連付けられたアクティビティを検出すると、ネットワーク マップにホストを追加します。Firepower Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

***表 1 : Firepower Management Center* モデル別のホスト制限**

Management Center モデル	ホスト
MC750	2,000
MC1500	50,000
FS2000	150,000
MC3500	300,000

Management Center モデル	ホスト
MC4000	600,000
仮想	50,000

ネットワーク マップに存在しないホストのコンテキスト データは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンス ホワイトリストを使用してホストのネットワーク コンプライアンスをモニタできない場合でも、ネットワーク マップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。

（注） システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて1つのホストとしてカウントされます。

ホスト制限への到達とホストの削除

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

マルチドメイン展開では、各リーフ ドメインに自身のネットワーク検出ポリシーがあります。したがって、各リーフ ドメインによって、システムが新しいホストを検出したときの独自の動作が決定されます。

関連トピック

ドメインのプロパティ
ネットワーク検出のデータ ストレージ設定

Firepower システムのユーザの制限

Firepower Management Center モデルにより、モニタできる個々のユーザ数が決まります。システムが新しいユーザのアクティビティを検出すると、そのユーザはFirepower Management CenterのUsersデータベースに追加されます。任意のアイデンティティ ソースを使用して、ユーザを検出できます。

検討するユーザ制限には 2 つのタイプがあります。

- 権限のあるユーザ数の制限。データベースに保存でき、アクセス制御に使用できる、アクセス制御されたユーザの数です。権限のあるユーザ データは、ユーザ エージェント、ISE/ISE-PIC、TS エージェント、およびキャプティブ ポータルによって収集されます。

- ユーザ総数の制限。データベースに保存できる、権限のあるユーザと権限のないユーザの数です。この制限には、すべての権限のあるユーザデータとトラフィックベースの検出を使用して収集された権限のないユーザ データが含まれます。

表 *2 : Firepower Management Center* モデル別のユーザ制限

Management Center モデル	権限のあるユーザ	ユーザ総数
MC750	2,000	2,000
MC1500	50,000	50,000
FS2000	64,000	150,000
MC3500	64,000	300,000
MC4000	64,000	600,000
仮想	50,000	50,000

制限に達してから、新しい、以前検出されなかったユーザをシステムが検出すると、アイデンティティ ソースに基づいてユーザ データに優先順位が付けられます。

- 新しいユーザが権限のないアイデンティティ ソースからである場合、ユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しいユーザを追加します。

（注） 展開に ASDM によって管理される ASA FirePOWER モジュールが含まれる場合、Firepower Management Center モデルに関係なく、最大 2,000 の権限のあるユーザを保存できます。

ヒント トラフィック ベースの検出を使用している場合、プロトコルによるユーザ ロギングを制限すると、ユーザ名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザを追加できないようにすることができます（モニタを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。