



ホストプロファイル

ここでは、ホストプロファイルの使用方法について説明します。

- ホストプロファイルの要件と前提条件 (1 ページ)
- ホストプロファイル (2 ページ)
- ホストプロファイルの基本ホスト情報 (4 ページ)
- ホストプロファイルのオペレーティングシステム (7 ページ)
- ホストプロファイルのサーバー (12 ページ)
- ホストプロファイルの Web アプリケーション (17 ページ)
- ホストプロファイルのホストプロトコル (19 ページ)
- ホストプロファイル内の侵害の兆候 (20 ページ)
- ホストプロファイルの VLAN タグ (20 ページ)
- ホストプロファイル内のユーザー履歴 (21 ページ)
- ホストプロファイル内のホスト属性 (21 ページ)
- ホストプロファイル内の許可リスト違反 (26 ページ)
- ホストプロファイルでのマルウェア検出 (27 ページ)
- ホストプロファイルの脆弱性 (28 ページ)
- ホストプロファイルのスキャン結果 (31 ページ)
- ホストプロファイルの履歴 (33 ページ)

ホストプロファイルの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者

- セキュリティアナリスト (Security Analyst)

ホストプロファイル

ホストプロファイルは、システムが1つのホストについて収集したすべての情報の完全なビューを提供します。ホストプロファイルにアクセスするには、以下のいずれかを実行します。

- 任意のネットワークマップビューから選択します。
- モニタ対象ネットワークでホストのIPアドレスを含む任意のイベントビューから選択します。

ホストプロファイルは、ホスト名やMACアドレスなど、検出されたホストやデバイスに関する基本的な情報を提供します。ライセンスやシステム設定によっては、ホストプロファイルは次の情報を提供することもできます。

- ホスト上で実行中のオペレーティングシステム
- ホスト上で実行中のサーバ
- ホスト上で実行中のクライアントとWebアプリケーション
- ホスト上で実行中のプロトコル
- ホスト上の侵害の兆候 (IOC) タグ
- ホスト上のVLANタグ
- ネットワーク上での過去24時間のユーザー活動
- ホストに関連するコンプライアンスallow違反
- ホストの最新のマルウェアイベント
- ホストに関連付けられている脆弱性
- ホストのNmapスキャン結果

プロファイルには、ホスト属性もリストされます。ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。例えば、以下を行うことができます。

- ホストが存在する建物を示すホスト属性を割り当てる
- ホストの重要度の属性を使用して、特定のホストのビジネス重要度を指定し、ホストの重要度に基づいて相関ポリシーとアラートを作成する

ホストプロファイルで、そのホストに適用されている既存のホスト属性を表示し、そのホスト属性値を変更できます。

パッシブ侵入防御展開の一部としてadaptive profile updatesを使用している場合、ホスト上のオペレーティングシステム、およびホストが実行しているサーバとクライアントのタイプに最も適合するように、システムがトラフィックを処理する方法を調整することができます。

オプションで、ホストプロファイルからNmapスキャンを実行し、ホストプロファイルのサーバ情報とオペレーティングシステムの情報を増やすことができます。Nmapスキャナはホストをアクティブに調査し、ホストを実行しているオペレーティングシステムおよびサーバの情報を取得します。スキャンの結果は、ホストのオペレーティングシステムおよびサーバーアイデンティティのリストに追加されます。

関連トピック

[ホストプロファイルの表示](#) (4 ページ)

ホストプロファイルの制限事項

利用できないホスト

ホストプロファイルは、ネットワーク上のすべてのホストでは使用できない可能性があります。考えられる原因は次のとおりです。

- タイムアウトしたため、ネットワーク マップからホストが削除された。
- ホストの制限に達した。
- ネットワーク検出ポリシーでモニタリングされないネットワークセグメントに、ホストが存在している。

利用できない情報

ホストプロファイルに表示される情報は、ホストのタイプ、および利用可能なホストの情報によって異なる可能性があります。

次に例を示します。

- 非 IP ベースのプロトコル (STP、SNAP、IPX など) を使用してシステムでホストを検出した場合、そのホストは MAC ホストとしてネットワーク マップに追加され、IP ホストに比べて使用できる情報はかなり少なくなります。
- システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイス データの違い](#)を参照)。

(VRF を実行している導入) 1 つの IP アドレスが複数のホストを表す場合がある

VRF を実行しているデバイスによってホストが報告された場合、1 つの IP アドレスが實際には複数のホストを表している可能性があります。VRF は、重複する IP アドレスを持つ複数のネットワークをモニターできます。そのため、同じ IP アドレスを異なるネットワークに存在させることができます。

ホストプロファイルの表示

手順

次の2つの選択肢があります。

- ネットワークマップで、プロファイルを表示するホストのIPアドレスをドリルダウンします。
- 任意のイベントビューで、[ホストプロファイル (Host Profile)]をクリックするか、プロファイルを表示するホストのIPアドレスの隣にある、[侵害を受けたホスト (Compromised Host)]をクリックします。

ホストプロファイルの基本ホスト情報

各ホストプロファイルは、検出されたホストまたは他のデバイスに関する基本情報を提供します。

次に、基本的なホストプロファイルのフィールドについて説明します。

ドメイン (Domain)

ホストに関連付けられているドメイン。

IPアドレス

ホストに関連付けられているすべてのIPアドレス (IPv4とIPv6の両方)。システムは、ホストに関連付けられているIPアドレスを検出し、サポートされている場合は、同じホストで使用される複数のIPアドレスをグループ化します。多くの場合、IPv6ホストには、少なくとも2つのIPv6アドレス（ローカルのみでルーティング可能なものと、グローバルにルーティング可能なもの）があり、その他にIPv4アドレスを持っていることがあります。IPv4専用ホストは、複数のIPv4アドレスを持っていることがあります。

ホストプロファイルは、そのホストに関連付けられている、検出されたすべてのIPアドレスを一覧で示します。可能な場合は、ルーティング可能なホストIPアドレスに、フラグアイコン、およびアドレスに関連付けられている地理情報データを表す国コードも含まれています。

デフォルトでは最初の3つのアドレスだけが表示されることに注意してください。[すべて表示 (Show All)]をクリックすると、ホストのすべてのアドレスが表示されます。

ホストネーム

ホストの完全修飾ドメイン名（わかる場合）。

NetBIOS 名 (NetBIOS Name)

ホストの NetBIOS 名 (使用できる場合)。Microsoft Windows ホストだけでなく Macintosh、Linux、または NetBIOS を使用するように設定されたその他のプラットフォームに NetBIOS 名を指定できます。たとえば、Samba サーバーとして設定されている Linux ホストに NetBIOS 名を指定します。

デバイス (ホップ数) (Device (Hops))

次のいずれかを行います。

- ホストが存在しているネットワークに関するレポート作成のデバイス (ネットワーク検出ポリシーで定義されている)、または
- ホストをネットワーク マップへ追加する NetFlow データを処理したデバイス

デバイス名の後に、ホストを検出したデバイスとホスト自身の間のネットワーク ホップの数が丸括弧で囲まれて表示されます。複数のデバイスで対象のホストを参照できる場合は、報告元のデバイスが太字で表示されます。

このフィールドが空白の場合は、次のいずれかになります。

- ホストがデバイスによってネットワーク マップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。または、
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

MAC アドレス (TTL) (MAC Addresses (TTL))

ホストについて検出された1つ以上のMACアドレスおよび関連付けられているNICベンダー。NICのハードウェアベンダーと現在の存続可能時間 (TTL) 値が括弧で囲まれて表示されます。

複数のデバイスが同じホストを検出した場合、Firewall Management Center には、どのデバイスがホストを報告したかに関係なく、ホストに関連付けられているすべての MAC アドレスと TTL 値が表示されます。

MAC アドレスが太字で表示されている場合、その MAC アドレスは、ARP および DHCP トライフィックを通じた検出により、IP アドレスに明確に関連付けられた、ホストの実際の/該当する/プライマリの MAC アドレスです。

太字フォントで表示されない MAC アドレスはセカンダリ アドレスなので、ホストの IP アドレスに明確に関連付けることはできません。たとえば、ファイアウォール デバイスは自身のネットワーク セグメント上のホストの MAC アドレスのみを取得できるため、トライフィックがファイアウォール デバイスが直接接続されていないネットワーク セグメントから発生している場合、監視されている MAC アドレス (ルータの MAC アドレス) は、ホストのセカンダリ MAC アドレスとして表示されます。

ホストタイプ (Host Type)

システムで検出されたデバイスのタイプ（ホスト、モバイルデバイス、ジェイルブレイクされたモバイルデバイス、ルータ、ブリッジ、NAT デバイス、またはロードバランサ）。

ネットワークデバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol (CDP) メッセージの分析。ネットワークのデバイスおよびそれらのタイプ (Cisco デバイスのみ) を特定できます。
- スパニングツリープロトコル (STP) の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロードバランサを識別します。
- モバイルデバイスを区別するためにシステムでは次の方法を使用します。
- モバイルデバイスのモバイルブラウザからの HTTP トрафィックのユーザー エージェント文字列の分析
- 特定のモバイルアプリケーションの HTTP トрафィックのモニタリング

デバイスがネットワークデバイスまたはモバイルデバイスとして識別されない場合は、ホストとして分類されます。

前回の検出 (Last Seen)

ホストのいずれかの IP アドレスが最後に検出された日時。

現在のユーザー (Current User)

このホストに最後にログインしたユーザー。

既存の現在のユーザーが権限のあるユーザーでない場合、ホストにログインしている権限を持たないユーザーは、現在のユーザーとして登録されるだけであることに注意してください。

表示 (View)

接続、検出、マルウェア、および侵入イベントデータのビューへのリンク。このリンクは、そのイベントタイプのデフォルトワークフローを使用し、ホストに関連するイベントを表示するよう制限されています。可能な場合は、これらのイベントには、ホストに関連付けられているすべての IP アドレスが含まれます。

ホスト プロファイルのオペレーティング システム

システムは、ホストで生成されたトライフィック内のネットワークおよびアプリケーションスタックを分析したり、User Agentでレポートされたホストデータを分析することによって、ホスト上で稼動しているオペレーティング システムのアイデンティティをパッシブに検出します。システムでは、他のソース（Nmap スキャナ、ホストの入力機能によりインポートされたアプリケーションデータ）のオペレーティング システムの情報も照合します。どのアイデンティティを使用するかを判断する場合、システムは、各アイデンティティのソース（発生源）に割り当てられている優先度を考慮します。デフォルトでは、ユーザ入力が最も高い優先度を持ち、以降は高い順にアプリケーションまたはスキャナソース、検出されたアイデンティティ、となります。

システムでは、オペレーティング システムの具体的な定義ではなく、全般的な定義を提供することがあります。これは、トライフィックおよび他のアイデンティティソースで、対象のアイデンティティを詳しく調べるための十分な情報が提供されないためです。システムは、できるだけ詳しい定義を使用するために、ソースの情報を照合します。

オペレーティング システムは、ホストの脆弱性リスト、およびホストを対象とするイベントの影響の相関関係に影響するため、オペレーティング システムの特定の情報を手動で入力することもできます。また、オペレーティング システムに対して、サービスパックやアップデートなどの修正ファイルが適用されたことを示すことも、修正ファイルによって対処された脆弱性を無効にすることもできます。

たとえば、システムでホストのオペレーティング システムが Microsoft Windows 2003 であると特定されたが、実際にはホストが Microsoft Windows XP Professional および Service Pack 2 を実行していることがわかっている場合、オペレーティング システムのアイデンティティを実際のとおりに設定することができます。より具体的なオペレーティング システムのアイデンティティを設定すると、ホストの脆弱性のリストの精度が向上するため、対象のホストに対する影響の相関関係が、より限定的かつ正確になります。

システムでホストに対するオペレーティング システム情報が検出され、その情報が、アクティブなソースによって提供されている現行のオペレーティング システムのアイデンティティと競合している場合、アイデンティティの競合が発生します。実際にアイデンティティの競合が発生している場合、システムは脆弱性と影響の相関関係の両方のアイデンティティを使用します。

ネットワーク検出ポリシーを設定して、NetFlow エクスポートによってモニタされるホストのネットワークマップに検出データを追加することができます。ただし、オペレーティング システムの ID を設定するためにホスト入力機能の使用を設定しない限り、これらのホストで使用可能なオペレーティング システムデータはありません。

オペレーティング システムを実行しているホストが、有効なネットワーク検出ポリシーのコンプライアンス allow リストに違反している場合、Firewall Management Center はオペレーティング システムの情報にallow リストの違反のマークを付けます。また、ジエイルブレイクされたモバイルデバイスが有効なallow リストに違反している場合、そのデバイスのオペレーティング システムの隣にアイコンが表示されます。

ホストのオペレーティングシステムのアイデンティティに対して、カスタム表示文字列を設定できます。この表示文字列は、ホストプロファイルで使用されます。



(注) あるホストについてオペレーティングシステムの情報を変更すると、ホストのコンプライアンス、およびコンプライアンスのallowリストが変わることの可能性があります。

ネットワークデバイスに対するホストプロファイルでは、[オペレーティングシステム (Operating Systems)]セクションのラベルが[システム (Systems)]に変わり、[ハードウェア (Hardware)]カラムが新しく表示されます。[システム (Systems)]の下にハードウェアプラットフォームの値が表示された場合、システムでは、ネットワークデバイスの背後で検出された1つ以上のモバイルデバイスを示します。モバイルデバイスはハードウェアプラットフォームの情報を持っていることも、持っていないこともあります。モバイルデバイスではないシステムではハードウェアプラットフォーム情報は検出されないことに注意してください。

次に、ホストプロファイルで表示されるオペレーティングシステムの情報フィールドについて説明します。

ハードウェア (Hardware)

モバイルデバイスのハードウェアプラットフォーム。

OS ベンダー/ベンダー (OS Vendor/Vendor)

オペレーティングシステムのベンダー。

OS 製品/製品 (OS Product/Product)

次の値のいずれかを指定します。

- すべてのソースから収集されたアイデンティティデータに基づいて、実行されている可能性が最も高いと判断されたオペレーティングシステム。
- [Pending] : システムがオペレーティングシステムをまだ識別しておらず、他に使用可能なアイデンティティデータがない場合。
- [unknown] : システムがオペレーティングシステムを識別できず、オペレーティングシステムに関して他に使用可能なアイデンティティデータがない場合。



(注) ホストのオペレーティングシステムをシステムで検出できない場合には、を参照してください。

OS バージョン/バージョン (OS Version/Version)

オペレーティング システムのバージョン。ホストがジェイルブレイクされたモバイルデバイスの場合、バージョンの後に括弧で囲まれて `Jailbroken` と示されます。

ソース (Source)

次の値のいずれかを指定します。

- [ユーザー (User)] : `user_name`
- [アプリケーション (Application)] : `app_name`
- [スキャナ (Scanner)] : `scanner_type` (Nmap またはその他のスキャナ)
- Firepower

システムでは、オペレーティング システムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

オペレーティング システム アイデンティティの表示

検出された、またはホストに追加された特定のオペレーティング システムのアイデンティティを表示することができます。システムはソースの優先度を使用して、ホストに対する現行のアイデンティティを判断します。アイデンティティのリストでは、現行のアイデンティティが太字で強調されます。

1 つのホストに対して複数のオペレーティング システムのアイデンティティが存在している場合のみ、[表示 (View)] が有効になっていることに注意してください。

手順

ステップ1 ホストプロファイルの[オペレーティング システム (Operating System)] または[オペレーティング システムの競合 (Operating System Conflicts)] セクションで [表示 (View)] をクリックします。

ステップ2 ホストプロファイルのオペレーティング システム (7ページ) の説明に従って情報を入力します。

ステップ3 必要に応じて、オペレーティング システムのアイデンティティの横にある[削除 (Delete)] (刪除) をクリックします。

(注)

シスコが検出したオペレーティング システムのアイデンティティは削除できません。

該当する場合は、このシステムは[オペレーティング システムのアイデンティティ情報 (Operating System Identity Information)] ポップアップ ウィンドウからアイデンティティを削除し、ホストプロファイルのオペレーティング システムの現在のアイデンティティを更新します。

現在のオペレーティングシステムのアイデンティティの設定

Firepower システム Web インターフェイスを使用して、ホストに対する現行のオペレーティングシステムのアイデンティティを設定できます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。ただし、オペレーティングシステムを編集した後で、ホストに対するオペレーティングシステムのアイデンティティの競合がシステムで検出されると、オペレーティングシステムの競合が発生します。競合が解決されるまで、両方のオペレーティングシステムが現行のものであるとみなされます。

手順

ステップ1 ホストプロファイルの [オペレーティングシステム (Operating System)] セクションで [編集 (Edit)] をクリックします。

ステップ2 ここでは次のオプションがあります。

- [OS 定義 (OS Definition)] ドロップダウンリストから [現在の定義 (Current Definition)] を選択して、ホスト入力によって現行のオペレーティングシステムのアイデンティティを確認して、手順 6 に進みます。
- [OS 定義 (OS Definition)] ドロップダウンリストから現行のオペレーティングシステムのアイデンティティのバリエーションを選択し、手順 6 に進みます。
- [OS 定義 (OS Definition)] ドロップダウンリストから [ユーザー定義 (User-Defined)] を選択して、手順 3 に進みます。

ステップ3 必要に応じて、[カスタム表示文字列を使用する (Use Custom Display String)] を選択し、[ベンダー文字列 (Vendor String)]、[製品文字列 (Product String)]、および [バージョン文字列 (Version String)] フィールドに表示するカスタム文字列を変更します。

ステップ4 必要に応じて、別のベンダーからのオペレーティングシステムに変更するには、[ベンダー (Vendor)] と [製品 (Product)] のドロップダウンリストから選択します。

ステップ5 必要に応じて、オペレーティングシステムの製品リリースレベルを設定するには、[メジャー (Major)]、[マイナー (Minor)]、[リビジョン (Revision)]、[ビルド (Build)]、[パッチ (Patch)]、および [拡張 (Extension)] ドロップダウンリストから選択します。

ステップ6 必要に応じて、オペレーティングシステムに対して修正ファイルが適用されたことを示す場合は、[修正の設定 (Configure Fixes)] をクリックします。

ステップ7 ドロップダウンリストから適用可能な修正を選択し、[追加 (Add)] をクリックします。

ステップ8 必要に応じて、[パッチ (Patch)] および [拡張 (Extension)] ドロップダウンリストを使用して、対象のパッチと拡張機能を追加します。

ステップ9 [完了 (Finish)] をクリックします。

関連トピック

[オペレーティングシステムのアイデンティティの競合 \(11 ページ\)](#)

オペレーティング システムのアイデンティティの競合

システムで検出された新しいアイデンティティと現行のアイデンティティが競合しており、そのアイデンティティが、スキャナやアプリケーション、ユーザなどのアクティブなソースによって提供されていた場合、オペレーティング システムのアイデンティティで競合が発生します。

ホスト プロファイルでは、競合状態のオペレーティング システムのアイデンティティのリストは太字で表示されます。

システムの Web インターフェイスを介して、アイデンティティの競合を解決し、ホストに対する現行のオペレーティング システムのアイデンティティを設定することができます。Web インターフェイスを介してアイデンティティを設定すると、他のすべてのアイデンティティ ソースが上書きされるため、このアイデンティティが、脆弱性の評価および影響の相関関係で使用されます。

競合するオペレーティング システム アイデンティティを現行に設定する

手順

ステップ1 ホスト プロファイルの [オペレーティング システム (Operating System)] セクションに移動します。

ステップ2 次の 2 つの選択肢があります。

- ホストのオペレーティング システムとして設定するオペレーティング システムのアイデンティティの隣にある、[現行にする (Make Current)] をクリックします。
 - アクティブなソースで、現行のアイデンティティとして使用しないアイデンティティが表示された場合は、使用しないアイデンティティを削除します。
-

オペレーティング システムのアイデンティティ競合の解決

手順

ステップ1 ホスト プロファイルの [オペレーティング システムの競合 (Operating System Conflicts)] セクションにある [解決 (Resolve)] をクリックします。

ステップ2 次の選択肢があります。

- [OS 定義 (OS Definition)] ドロップダウンリストから [現在の定義 (Current Definition)] を選択して、ホスト入力によって現行のオペレーティング システムのアイデンティティを確認して、手順 6 に進みます。

■ ホストプロファイルのサーバー

- ・[OS 定義 (OS Definition)] ドロップダウンリストから、競合しているオペレーティングシステムのアイデンティティのいずれかのバリエーションを選択して、手順 6 に進みます。
- ・[OS 定義 (OS Definition)] ドロップダウンリストから [ユーザー定義 (User-Defined)] を選択して、手順 3 に進みます。

ステップ3 必要に応じて、[カスタム表示文字列の使用 (Use Custom Display String)] を選択して、表示するカスタム文字列を [ベンダー文字列 (Vendor String)]、[製品文字列 (Product String)]、および [バージョン文字列 (Version String)] フィールドに入力します。

ステップ4 必要に応じて、別のベンダーからのオペレーティングシステムに変更するには、[ベンダー (Vendor)] と [製品 (Product)] のドロップダウンリストから選択します。

ステップ5 必要に応じて、オペレーティングシステムの製品リリース レベルを設定するには、[メジャー (Major)]、[マイナー (Minor)]、[リビジョン (Revision)]、[ビルド (Build)]、[パッチ (Patch)] および [拡張 (Extension)] ドロップダウンリストから選択します。

ステップ6 必要に応じて、オペレーティングシステムに対して修正ファイルが適用されたことを示す場合は、[修正の設定 (Configure Fixes)] をクリックします。

ステップ7 適用した修正ファイルを、修正ファイルリストに追加します。

ステップ8 [完了 (Finish)] をクリックします。

ホストプロファイルのサーバー

ホストプロファイルのサーバセクションでは、監視対象ネットワーク上のホストで検出されるか、エクスポートされたNetFlow レコードから追加されるか、スキャナまたはホスト入力機能のようなアクティブなソースを介して追加されるサーバを例挙します。

リストは 1 つのホストにつき最大 100 台のサーバを表示します。100 個の制限に達すると、ホストからサーバを削除するか、またはサーバがタイムアウトになるまで、いずれかのソースの新しいサーバ情報は、アクティブであってもパッシブであっても廃棄されます。

Nmap を使用してホストをスキャンすると、オープンな TCP ポート上で稼動している、以前に検出されなかったサーバの結果が Nmap によって Servers リストに追加されます。Nmap スキャンを実行した場合、または Nmap の結果をインポートした場合、ホストプロファイルに拡張可能な [スキャン結果 (Scan Results)] セクションも表示され、Nmap スキャンによってホスト上で検出されたサーバ情報が示されます。さらに、ネットワークマップからホストが削除されると、ホストのそのサーバに対する Nmap スキャンの結果は廃棄されます。



(注) システムは、エクスポートされたNetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます（[NetFlow データと管理対象デバイスデータの違い](#)を参照）。

ホストプロファイルでサーバーを使用するためのプロセスは、ユーザーがプロファイルにアクセスする方法によって異なります。

- ネットワークマップを介したドリルダウンによりホストプロファイルにアクセスする場合は、サーバーの名前が太字で強調されて、サーバーの詳細が表示されます。ホストの他のサーバーの詳細を表示する場合は、対象のサーバー名の隣にある[表示 (View)] (◎) をクリックします。
- 他の方法でホストプロファイルにアクセスする場合は、[サーバー (Servers)] セクションを展開し、詳細を表示するサーバーの隣にある[表示 (View)] (◎) をクリックします。



(注) ホストが、有効な相関ポリシーにおけるコンプライアンスのallowリストに違反しているサーバーを実行している場合、Firewall Management Center は非準拠サーバーに、allowリストの [違反 (Violation)] のマークを付けます。

次に、[Servers リスト (Servers list)] の列について説明します。

プロトコル

サーバが使用するプロトコルの名前。

[ポート (Port)]

サーバが実行されているポート。

アプリケーションプロトコル (Application Protocol)

次のいずれかになります。

- アプリケーションプロトコルの名前
- [保留中 (pending)] : システムで、いずれかの理由でアプリケーションプロトコルをポジティブまたはネガティブに識別できない場合
- [未知 (unknown)] : 既知のアプリケーションプロトコルのフィンガープリントに基づいてシステムでアプリケーションプロトコルを識別できない場合、または（対応するサーバは追加せずに、ポート情報での脆弱性を追加することにより）ホストの入力を介してサーバが追加された場合

アプリケーションプロトコルの名前にマウスを重ねると、タグが表示されます。

ベンダーおよびバージョン (Vendor and Version)

システム、Nmap、または他のアクティブなソースで識別されたベンダーとバージョン、またはホストの入力機能を介して取得したベンダーとバージョン。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホストプロファイルのサーバーの詳細

Firewall Management Center は、1 つのサーバについてパッシブに検出されるアイデンティティを最大 16 個表示します。パッシブな検出ソースには、ネットワーク検出データおよび NetFlow レコードが含まれます。システムで、このサーバの複数のベンダーまたはバージョンを検出した場合、サーバは複数のパッシブなアイデンティティを持つことができます。たとえば、複数の Web サーバーで同じバージョンのサーバー ソフトウェアが実行されていない場合、管理対象デバイスと Web サーバーフーム間にロード バランサがあると、システムでは HTTP について複数のパッシブアイデンティティが識別されることがあります。Firewall Management Center は、アクティブなソース（ユーザー入力、スキャナ、その他のアプリケーションなど）からのサーバー アイデンティティの数を制限することはありません。

Firewall Management Center は現行のアイデンティティを太字で表示します。システムでは、さまざまな目的でサーバーの現行のアイデンティティが使用されます。このような目的には、1 つのホストに対する脆弱性の割り当て、影響の評価、ホストプロファイルの証明書およびコンプライアンス allow リストに対して記載された相関ルールの評価などがあります。

サーバーの詳細には、選択されたサーバーについて知られている、更新済みのサブサーバー情報が表示されることもあります。

サーバの詳細にサーバのバナーが表示されることもあります。これは、ホストプロファイルからサーバを表示したときに、サーバの詳細の下に表示されます。サーバのバナーは、サーバを識別するのに役立つサーバに関する追加情報を提供します。攻撃者がサーバのバナー文字列を意図的に変更した場合、システムは誤ったアイデンティティが示されたサーバを識別または検出できません。サーバのバナーには、そのサーバについて検出された最初のパケットの最初の 256 文字が表示されます。この情報は、サーバがシステムによって最初に検出されたときに一度だけ収集されます。バナーの内容は 2 列で表示されます。左側の列は 16 進表記で示され、右側の列は対応する ASCII 表記で示されます。



(注) サーバーのバナーを表示するには、ネットワーク検出ポリシーで [バナーのキャプチャ (Capture Banners)] チェックボックスをオンにする必要があります。このオプションはデフォルトでは無効になっています。

ホストプロファイルのサーバの詳細セクションには、次の情報が含まれています。

プロトコル

サーバが使用するプロトコルの名前。

[ポート (Port)]

サーバが実行されているポート。

ヒット数 (Hits)

管理対象デバイスまたは Nmap スキャナによってサーバーが検出された回数。ホストの入力によってインポートされたサーバについては、システムがそのサーバについてトラフィックを検出しない場合、検出回数は 0 になります。

前回の使用 (Last Used)

サーバが最後に検出された日時。システムで対象のサーバについて新しいトライフィックを検出しない場合、ホスト入力のデータが最後に使用された時間は、データの最初のインポート時間を反映しています。ホストの入力機能を介してインポートされたスキャナおよびアプリケーションのデータは、Firewall Management Center の設定に応じてタイムアウトしますが、Firewall Management Center の Web インターフェイスを介したユーザ入力の場合はタイムアウトしません。

アプリケーション プロトコル (Application Protocol)

サーバによって使用されるアプリケーション プロトコルの名前 (既知の場合)。

[ベンダー (Vendor)]

サーバのベンダー。ベンダーがわからない場合、このフィールドは表示されません。

バージョン (Version)

サーバのバージョン。バージョンがわからない場合、このフィールドは表示されません。

ソース (Source)

次の値のいずれかを指定します。

- [ユーザー (User)] : user_name
- [アプリケーション (Application)] : app_name
- [スキャナ (Scanner)] : scanner_type (Nmap または他のスキャナ)
- システムで検出されたアプリケーションの場合、Firepower、Firepower Port Match、またはFirepower Pattern Match
- NetFlow レコードからネットワーク マップに追加されたサーバの場合、NetFlow

システムでは、サーバーのアイデンティティを判断するために、複数のソースのデータを統合することができます。

サーバ詳細情報の表示

手順

ホストプロファイルの[サーバー (Servers)]セクションで、サーバーの横にある[表示 (View)] (oculars) をクリックします。

サーバーのアイデンティティの編集

ホスト上のサーバーのアイデンティティ設定を手動で更新し、修正ファイルによって対処された脆弱性を削除するために、ホストに適用した何らかの修正ファイルを設定することができます。サーバーのアイデンティティを削除することもできます。

アイデンティティを削除した場合、削除したアイデンティティが唯一のアイデンティティであっても、サーバーは削除されません。アイデンティティを削除すると、[サーバーの詳細 (Server Detail)] ポップアップ ウィンドウからアイデンティティが削除されます。可能な場合は、ホストプロファイルでそのサーバーの現行のアイデンティティを更新します。

シスコ管理対象デバイスによって追加されたサーバーのアイデンティティは、編集または削除できません。

手順

-
- ステップ1** ホストプロファイルの [サーバー (Servers)] セクションに移動します。
 - ステップ2** [表示 (View)] をクリックし、[サーバーの詳細 (Server Detail)] ポップアップ ウィンドウを開きます。
 - ステップ3** サーバーのアイデンティティを削除するには、削除するサーバーアイデンティティの隣にある [削除 (Delete)] (⊖) をクリックします。
 - ステップ4** サーバーのアイデンティティを変更するには、サーバーリストでサーバーの隣にある [編集 (Edit)] (⊖) をクリックします。
 - ステップ5** 次の2つの選択肢があります。
 - ・[サーバータイプの選択 (Select Server Type)] ドロップダウンリストから現行の定義を選択します。
 - ・[サーバータイプの選択 (Select Server Type)] ドロップダウンリストからサーバータイプを選択します。
 - ステップ6** 必要に応じて、対象のサーバータイプのベンダーと製品のみを表示する場合は、[サーバータイプ別に制限 (Restrict by Server Type)] チェックボックスをオンにします。
 - ステップ7** オプションでサーバーの名前とバージョンをカスタマイズするには、[カスタム表示文字列の使用 (Use Custom Display String)] を選択し、[ベンダー文字列 (Vendor String)] と [バージョン文字列 (Version String)] に入力します。
 - ステップ8** [製品マッピング (Product Mappings)] セクションで、使用するオペレーティングシステム、製品、およびバージョンを選択します。
 - 例 :**
たとえば、サーバーを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。
 - ステップ9** サーバーの修正が適用されていることを示す場合は、[修正の設定 (Configure Fixes)] をクリックして、そのサーバーに適用するパッチを修正リストに追加します。

ステップ10 [完了 (Finish)] をクリックします。

サーバー アイデンティティの競合の解決

アプリケーションやスキャナなどのアクティブなソースが、サーバーのアイデンティティデータをホストへ追加したときに、サーバー アイデンティティの競合が発生します。その後で、システムはサーバー アイデンティティの競合を示しているポートのトラフィックを検出します。

手順

ステップ1 ホスト プロファイルで、[サーバー (Servers)] セクションに移動します。

ステップ2 サーバーの横にある解決をクリックします。

ステップ3 [サーバータイプの選択 (Select Server Type)] ドロップダウンリストからサーバーのタイプを選択します。

ステップ4 必要に応じて、対象のサーバータイプのベンダーと製品のみを表示する場合は、[サーバータイプ別に制限 (Restrict by Server Type)] チェックボックスをオンにします。

ステップ5 必要に応じて、サーバーの名前とバージョンをカスタマイズする場合は、[カスタム表示文字列の使用 (Use Custom Display String)] を選択して、[ベンダー文字列 (Vendor String)] と [バージョン文字列 (Version String)] を入力します。

ステップ6 [製品マッピング (Product Mappings)] セクションで、使用するオペレーティングシステム、製品、およびバージョンを選択します。

例：

たとえば、サーバーを Red Hat Linux 9 にマップする場合は、ベンダーとして [Redhat, Inc.] を、製品として [Redhat Linux] を選択し、バージョンとして [9] を選択します。

ステップ7 サーバーの修正が適用されていることを示す場合は、[修正の設定 (Configure Fixes)] をクリックして、そのサーバーに適用するパッチを修正リストに追加します。

ステップ8 [完了 (Finish)] をクリックします。

ホスト プロファイルの Web アプリケーション

ホスト プロファイルの [Web アプリケーション (Web Application)] セクションには、ネットワーク内のホスト上で動作していることをシステムが識別したクライアントと Web アプリケーションが表示されます。システムでは、パッシブ検出ソースとアクティブ検出ソースの両方から取得されるクライアントと Web アプリケーションの情報を識別できます。ただし、NetFlow レコードから追加されたホストに関する情報は一部しか取得することができません。

このセクションには、ホスト上で検出されたアプリケーションの製品とバージョン、使用できるクライアントまたはWebアプリケーションの情報、アプリケーションが最後に使用中であると検出された時間などの詳細情報が表示されます。

ホスト上で稼動している最大16個のクライアントが、このセクションに表示されます。16個の制限に達すると、ユーザーがホストからクライアントアプリケーションを削除するか、または非アクティブである（クライアントがタイムアウトしている）ためにシステムによってホストプロファイルからクライアントが削除されるまで、新しいクライアント情報は、どのソースのものであるか、アクティブかパッシブかにかかわらず、廃棄されます。

また、検出されたそれぞれのWebブラウザについては、アクセスされた最初の100個のWebアプリケーションが表示されます。この制限に達すると、ブラウザに関連付けられている新しいWebアプリケーションは、どのソースのものであるか、アクティブかパッシブかにかかわらず、次の条件を満たすまで廃棄されます。

- Webブラウザのクライアントアプリケーションがタイムアウトになる、または
- ユーザーが、Webアプリケーションに関連付けられているアプリケーション情報をホストプロファイルから削除する

ホストが、有効な相関ポリシーにおけるコンプライアンスallowリストに違反しているアプリケーションを実行している場合、Firepower Management Centerは非準拠サーバーに、allowリストの違反のマークを付けます。



ヒント

ホスト上の特定のアプリケーションに関連付けられている接続イベントを分析するには、アプリケーションの隣にある**ロギング** (目) をクリックします。接続イベントに対する優先ワークフローの最初のページが表示され、ホストのIPアドレスの他、アプリケーションのタイプ、製品、およびバージョンによって制限された接続イベントが示されます。接続イベントに対する優先ワークフローがない場合、ワークフローを選択する必要があります。

次に、ホストプロファイルに表示されるアプリケーション情報について説明します。

アプリケーションプロトコル (Application Protocol)

アプリケーション（HTTPブラウザ、DNSクライアントなど）で使用されるアプリケーションプロトコルを表示します。

クライアント (Client)

ペイロードから派生したクライアント情報。この情報は、Firepowerシステムが識別するか、Nmapがキャプチャするか、またはホスト入力機能によって取得されます。有効なソースで識別が行われなかった場合、フィールドは空白になります。

バージョン (Version)

クライアントのバージョンを表示します。

Web アプリケーション

Web ブラウザの場合は、http トライフィックでシステムによって検出されたコンテンツ。Web アプリケーションの情報は、Firepower システムによって識別された、Nmap によってキャプチャされた、他のアクティブなソースによって取得された、またはホストの入力機能を介して取得された特定のタイプのコンテンツ（WMV や QuickTime など）を表します。有効なソースで識別が行われなかった場合、フィールドは空白になります。

ホスト プロファイルから Web アプリケーションを削除する

ホスト上で稼働していないことが判明しているアプリケーションを削除するには、ホスト プロファイルからアプリケーションを削除します。ホストからアプリケーションを削除すると、そのホストにallowリストのコンプライアンスが適用されることがあります。



(注) システムでアプリケーションが再検出されると、アプリケーションはネットワークマップおよびホスト プロファイルに再度追加されます。

手順

ステップ1 ホスト プロファイルで、[アプリケーション (Applications)] セクションに移動します。

ステップ2 削除するアプリケーションの横にある[削除 (Delete)] (Delete icon) をクリックします。

ホスト プロファイルのホスト プロトコル

各ホスト プロファイルには、ホストに関連付けられているネットワーク トライフィックで検出されたプロトコルに関する情報が含まれています。この情報には次のものが含まれます。

プロトコル

ホストが使用するプロトコルの名前。

層 (Layer)

プロトコルを実行しているネットワーク層 (Network または Transport)。

ホスト プロファイルに表示されているプロトコルが、有効な相関ポリシーのコンプライアンス allow リストに違反する場合、Firewall Management Center は非準拠プロトコルに、allow リストの違反 のマークを付けます。

ホスト プロファイルに、ホスト上で実行していないことがわかっているプロトコルがリストされている場合は、これらのプロトコルを削除できます。ホストからプロトコルを削除すると、ホストがコンプライアンス allow リストに準拠する可能性があります。

■ ホストプロファイルからプロトコルを削除する



(注) システムでプロトコルが再検出されると、プロトコルはネットワークマップおよびホストプロファイルに再度追加されます。

ホストプロファイルからプロトコルを削除する

手順

ステップ1 ホストプロファイルの[プロトコル(Protocols)]セクションに移動します。

ステップ2 削除するプロトコルの横にある[削除>Delete]()をクリックします。

ホストプロファイル内の侵害の兆候

システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、セキュリティインテリジェンス、接続イベント、ファイルまたはマルウェアイベント）との関連性を示します。イベントデータの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。

ホストプロファイルの[侵害の兆候(Indications of Compromise)]セクションには、ホストのすべての侵害の兆候のタグが表示されます。

侵害の兆候にタグを付けるように設定するには、Cisco Secure Firewall Management Center デバイス構成ガイドの「Enabling Indications of Compromise Rules」を参照してください。

侵害の兆候についての作業の詳細については、侵害の兆候データとそのトピックのサブトピックを参照してください。

ホストプロファイルのVLANタグ

ホストが仮想LAN（VLAN）のメンバである場合、ホストプロファイルの[VLANタグ(VLAN Tag)]セクションが表示されます。

物理ネットワーク機器は、多くの場合にVLANを使用して、さまざまなネットワークブロックから論理ネットワークセグメントを作成します。システムは802.1q VLANタグを検出し、それに対して以下の情報を表示します。

- [VLAN ID]は、ホストがメンバであるVLANを表します。これは、802.1q VLANの場合、0～4095の任意の整数となります。

・[タイプ (Type)] は、VLAN タグが含まれている、カプセル化されたパケットを表します。値は Ethernet または Token Ring となります。

・[優先順位 (Priority)] は、VLAN タグの優先度を表します。これは 0 ~ 7 の任意の整数で、7 は最も高い優先度です。

VLAN タグがパケット内でネスト構造になっている場合、システムは最も内側の VLAN タグを処理し、Firewall Management Center は最も内側の VLAN タグを表示します。システムは、ARP および DHCP トライフィックを通じて識別される MAC アドレスのみの VLAN タグ情報を収集し、これらのタグを表示します。

たとえば全体がプリンタで構成されている VLAN があり、システムがこの VLAN で Microsoft Windows 2000 のオペレーティング システムを検出した場合などは、VLAN タグ情報が有用です。VLAN 情報により、システムは正確性の高いネットワーク マップを生成できるようになります。

ホスト プロファイル内のユーザー履歴

ホスト プロファイルのユーザー履歴の部分には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。一般的なユーザーは夕方にログオフし、また他のユーザーとホストのリソースを共有することができます。電子メールのチェックなどの目的で行われる定期的なログインの要求は、短い標準の棒で示されます。ユーザーのアイデンティティリストは棒グラフで提示され、ユーザー ログインが検出されたタイミングを示します。権限のないログインの場合は、棒グラフがグレーになっていることに注意してください。

システムは、ホストに対する権限のないユーザー ログインを、そのホストの IP アドレスに関連付けるため、そのユーザーはそのホストのユーザー履歴に表示されます。ただし、権限のあるユーザー ログインが同じホストで検出された場合、その権限のあるユーザー ログインに関連付けられているユーザが、そのホストの IP アドレスとの関連付けを引き継ぐため、新しい権限のないユーザー ログインがそのホストの IP アドレスとのそのユーザの関連付けを壊すことはありません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、リストにはこのホストへのログインに失敗したユーザーが含まれます。

ホスト プロファイル内のホスト属性

ホスト属性を使用して、ネットワーク環境にとって重要な方法でホストを分類することができます。Firepower システムには以下の 3 つのタイプの属性があります。

- ・定義済みホスト属性
- ・コンプライアンスの *allow* リストのホスト属性
- ・ユーザー定義ホスト属性

定義済みホスト属性を設定後、またはユーザ定義ホスト属性を作成後は、ホスト属性の値を割り当てる必要があります。

■ 定義済みホスト属性



(注)

ホスト属性は、どのドメインレベルでも定義できます。現在のドメインと先祖ドメインで作成されたホスト属性を割り当てることができます。

定義済みホスト属性

Firewall Management Center には、2 つの定義済みホスト変数が用意されています。

ホストの重要度 (Host Criticality)

特定のホストの業務の重要性を指定し、ホストの重要性に応じて相関ポリシーの応答を調整するには、この属性を使用します。たとえば、業務にとって組織のメールサーバが一般的なユーザワークステーションよりも重要であるとみなしている場合は、メールサーバと業務に重要なその他のデバイスに [高 (High)] の値を割り当て、他のホストには [中 (Medium)] または [低 (Low)] の値を割り当てることができます。その上で、影響を受けるホストの重要度に基づいて異なるアラートを起動する相関ポリシーを作成できます。

注記 (Notes)

他のアナリストに確認してもらいたいホストに関する情報を記録するには、このホスト固有の属性を使用します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンのテスト用オペレーティングシステムが搭載されている場合、[注記 (Notes)] 属性を使用して、システムは意図的にパッチを適用していないことを明示できます。

許可リストのホスト属性

ユーザーが作成するコンプライアンス allow リストごとに、各allowリストと同じ名前でホスト属性が自動的に作成されます。allowリストのホスト属性に設定可能な値は、次のとおりです。

- ・準拠 (Compliant) : allowリストに準拠しているホストを識別します。
- ・非準拠 (Non-Compliant) : allowリストに違反しているホストを識別します。
- ・未評価 (Not Evaluated) : allowリストの有効な対象ではないホスト、または何らかの理由で評価されていないホストを識別します。

allowリストのホスト属性の値を編集したり、allowリストのホスト属性を削除したりすることはできません。

ユーザ定義のホスト属性

定義済みのホスト属性またはコンプライアンス allow リストのホスト属性で使用されている基準と異なる基準を使用してホストを識別する場合、ユーザ定義のホスト属性を作成することができます。例えば、以下を行うことができます。

- ホストに対してファシリティ コード、市町村、部屋番号などの物理的なロケーション ID を割り当てます。
- 特定のホストを担当するシステム管理者を示す担当者 ID を割り当てます。ホストに関連する問題が検出された場合、相関ルールとポリシーを作成して、適切なシステム管理者にアラートを送信することができます。
- ホストの IP アドレスに基づいて、事前定義されたリストからホストへ自動的に値を割り当てます。この機能は、ネットワーク上にホストが初めて表示されたときに、その新しいホストへ値を割り当てるために役立ちます。

ユーザ定義のホスト属性は、ホストプロファイルのページに表示されます。ここでホストごとに値を割り当てるすることができます。次のことも実行できます。

- 相関ポリシーと検索でホスト属性を使用します。
- イベントのホスト属性テーブルビューで属性を表示して、それに基づいてレポートを生成します。

ユーザ定義のホスト属性として、次のタイプのいずれか 1 つを使用できます。

テキスト (Text)

ホストに対してテキスト文字列を手動で割り当てるすることができます。

整数 (Integer)

正の整数の範囲の最初の数と最後の数を指定してから、ホストに対してこれらの数の 1 つを手動で割り当てるすることができます。

リスト (List)

文字列値のリストを作成してから、ホストに対してこの値のいずれかを割り当てるすることができます。また、ホストの IP アドレスに基づいて、ホストに対して値を自動的に割り当てるすることもできます。

複数の IP アドレスを持つホストの 1 つの IP アドレスに基づいて値を自動的に割り当てる場合、これらの値は、ホストに関連付けられているすべてのアドレスに適用されます。[ホスト属性 (Host Attributes)] テーブルを表示する場合は、このことに留意してください。

リストの値を自動的に割り当てる場合は、リテラルの IP アドレスではなくネットワークオブジェクトの使用を検討してください。このアプローチによって保守容易性を向上でき、特にマルチドメイン展開で有効です。これは、マルチドメイン展開でオーバーライドが有効になったオブジェクトを使用すると、子孫ドメインの管理者が先祖ドメインの設定を自分のローカル環境に合わせて調整できるためです。マルチドメイン展開では、子孫ドメインで重複した IP アドレスを使用している場合に意図しないホストに一致するのを避けるために、先祖ドメインレベルで自動割り当てリストを定義する場合は注意してください。

URL

ホストに対して手動で URL の値を割り当てるすることができます。

■ テキストまたは URL に基づくホスト属性の作成

ユーザ一定義のホスト属性を削除すると、その属性が使用されているすべてのホストプロファイルから削除されます。

テキストまたは URL に基づくホスト属性の作成

手順

ステップ1 [分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ホスト属性 (Host Attributes)] を選択します。

ステップ2 [ホスト属性管理 (Host Attribute Management)] をクリックします。

ステップ3 [属性の作成 (Create Attribute)] をクリックします。

ステップ4 名前を入力します。

ステップ5 [ユーザ定義のホスト属性 \(22 ページ\)](#) の説明に従って作成する属性の [タイプ (Type)] を選択します。

ステップ6 [保存 (Save)] をクリックします。

整数ベースのホスト属性の作成

整数ベースのホスト属性を定義する場合は、その属性が受け入れる数値の範囲を指定する必要があります。

手順

ステップ1 [分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ホスト属性 (Host Attributes)] を選択します。

ステップ2 [ホスト属性管理 (Host Attribute Management)] をクリックします。

ステップ3 [属性の作成 (Create Attribute)] をクリックします。

ステップ4 名前を入力します。

ステップ5 [ユーザ定義のホスト属性 \(22 ページ\)](#) の説明に従って、作成する属性の [タイプ (Type)] を選択します。

ステップ6 [最小 (Min)] フィールドに、ホストに対して割り当てる能够範囲の最小の整数値を入力します。

ステップ7 [Max] フィールドに、ホストに対して割り当てる能够範囲の最大の整数値を入力します。

ステップ8 [保存 (Save)] をクリックします。

リストベースのホスト属性の作成

リストベースのホストの属性を定義する場合は、リストに対してそれぞれの値を提供する必要があります。これらの値には、英数字、スペース、および記号を含めることができます。

手順

-
- ステップ1** [分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ホスト属性 (Host Attributes)] を選択します。
- ステップ2** [ホスト属性管理 (Host Attribute Management)] をクリックします。
- ステップ3** [属性の作成 (Create Attribute)] をクリックします。
- ステップ4** 名前を入力します。
- ステップ5** [ユーザ定義のホスト属性 \(22 ページ\)](#) の説明に従って、作成する属性の [タイプ (Type)] を選択します。
- ステップ6** リストに値を追加するには、[値の追加 (Add Value)] をクリックします。
- ステップ7** [名前 (Name)] フィールドに、追加する最初の値を入力します。
- ステップ8** オプションで、ホストに追加した属性値を自動で割り当てるには、[ネットワークを追加 (Add Networks)] をクリックします。
- ステップ9** [値 (Value)] ドロップダウン リストから、追加した値を選択します。
- ステップ10** [IP アドレス (IP Address)] および [ネットマスク (Netmask)] フィールドに、この値を自動的に割り当てる IP アドレスのブロックを表す IP アドレスとネットワーク マスク (IPv4) を入力します。
- ステップ11** リストにさらに値を追加して、IP アドレス ブロックの範囲内の新しいホストにこれらの値を自動的に割り当てるには、手順 6 ~ 10 を繰り返します。
- ステップ12** [保存 (Save)] をクリックします。
-

ホスト属性値の設定

事前定義またはユーザ定義のホスト属性に値を設定できます。システムによって生成されたコマンドライアンス allow リストのホスト属性値は設定できません。

手順

-
- ステップ1** 変更するホストプロファイルを開きます。
- ステップ2** [属性 (Attributes)] セクションで、[属性の編集 (Edit Attributes)] をクリックします。
- ステップ3** 必要に応じて、属性を更新します。

■ ホストプロファイル内の許可リスト違反

ステップ4 [保存 (Save)] をクリックします。

ホストプロファイル内の許可リスト違反

コンプライアンスallowリスト（またはallowリスト）は一連の基準で、ユーザーはこれを使用して、特定のサブネット上での実行が許可されるオペレーティングシステム、アプリケーションプロトコル、クライアント、Webアプリケーション、およびプロトコルを指定することができます。

アクティブな相関ポリシーにallowリストを追加した場合に、システムでallowリストに違反しているホストがあることが検出されると、Firewall Management Centerはallowリストのイベント（相関イベントの特別な種類）をデータベースに記録します。これらのallowリストイベントはそれぞれallowリスト違反に関連付けられます。これには、特定のホストがどのようにallowリストに違反しているか、および違反している理由が含まれています。あるホストが1つ以上のallowリストに違反している場合、ホストプロファイルにおいて、2つの方法でこれらの違反を参照することができます。

ホストプロファイルには最初に、ホストに関連付けられている個々のallowリストの違反がすべて一覧表示されます。

次に、ホストプロファイルにおけるallowリスト違反の説明が続きます。

タイプ

違反のタイプ（つまり、違反がオペレーティングシステム、アプリケーション、サーバ、またはプロトコルの非準拠の結果として生じたかどうか）。

理由

違反についての特別な理由。たとえば、Microsoft Windowsのホストのみを許可するallowリストがある場合、ホストプロファイルには、ホストで稼働している現行のオペレーティングシステム（Linux Linux 2.4、2.6など）が表示されます。

許可リスト

違反に関連付けられているallowリストの名前。

次に、オペレーティングシステム、アプリケーション、プロトコル、およびサーバーに関連付けられているセクションで、Firewall Management Centerが、非準拠の要素にallowリストの [違反 (Violation)] のマークを付けます。たとえば、Microsoft Windowsホストのみを許可するようなallowリストでは、ホストプロファイルは、ホストのオペレーティングシステム情報の隣にallowリスト違反のアイコンを表示します。



（注） ホストのプロファイルを使用すると、コンプライアンスallowリストの共有ホストプロファイルを作成することができます。

共有許可リストホストプロファイルの作成

コンプライアンスallowリストの共有ホストプロファイルは、複数のallowリストで、ターゲットホスト上で実行を許可されるオペレーティングシステム、アプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルを指定します。つまり、複数のallowリストを作成するが、同じホストプロファイルを使用して複数のallowリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有ホストプロファイルを使用します。

既知の IP アドレスが割り当てられている任意のホストのホストプロファイルを使用して、コンプライアンスallowリストで使用できる共有ホストプロファイルを作成することができます。ただし、システムでホストのオペレーティングシステムをまだ特定していない場合は、個々のホストのホストプロファイルに基づいて共有ホストプロファイルを作成することはできないことに注意してください。

手順

ステップ1 ホストプロファイルで、[許可リスト (Allow List) プロファイルの生成 (Generate White List Profile)] をクリックします。

ステップ2 特別なニーズに応じて、共有ホストプロファイルを変更し、保存します。

関連トピック

[許可リスト ホストプロファイルの作成](#)

ホスト プロファイルでのマルウェア検出

[最後に検出されたマルウェア (Most Recent Malware Detections)] セクションには、ホストがマルウェア ファイルを送信または受信した、最近のマルウェア イベントが最大 100 個表示されます。ホスト プロファイルには、ネットワークベースのマルウェア イベント (マルウェア 防御によって生成されたもの) とエンドポイントベースのマルウェア イベント (エンドポイント向け AMP によって生成されたもの) の両方のリストが示されます。

ファイルが遡ってマルウェアと識別されたファイルイベントにホストが関係している場合、ファイルが送信された元のイベントは、マルウェアの特定が行われた後で、マルウェアの検出リストに表示されます。マルウェアとして識別されたファイルが、マルウェアではないと遡って判断された場合、そのファイルに関するマルウェア イベントはリストには表示されなくなります。たとえば、ファイルの性質が `Malware` であり、これが `Clean` に変わった場合、そのファイルのイベントは、ホスト プロファイル上のマルウェア検出リストから削除されます。

ホスト プロファイルでマルウェアの検出を確認する際には、[マルウェア (Malware)] をクリックして、そのホストのマルウェア イベントを確認できます。

次に、ホスト プロファイルの [最新のマルウェア検出 (Most Recent Malware Detections)] セクションの列について説明します。

時刻 (Time)

イベントが生成された日時。

ファイルがマルウェアであると遡って特定されたイベントでは、これはマルウェアが特定された時刻ではなく、元のイベントの時刻であることに注意してください。

[ホストロール (Host Role)]

検出されたマルウェアの伝送におけるホストのロール（送信側または受信側）。エンドポイント向けAMPによって生成されたマルウェアイベント（「エンドポイントベースのマルウェアイベント」）の場合、ホストは常に受信者になります。

[脅威名 (Threat Name)]

検出されたマルウェアの名前。

File Name

マルウェアファイルの名前。

[ファイルタイプ (File Type)]

ファイルのタイプ（PDFやMSEXEなど）。

ホストプロファイルの脆弱性

ホストプロファイルの [脆弱性 (Vulnerabilities)] セクションには、ホストに影響を与える脆弱性が示されます。これらの脆弱性は、システムがホスト上で検出したオペレーティングシステム、サーバ、およびアプリケーションに基づきます。

ホストのオペレーティングシステムのアイデンティティ、またはホスト上のアプリケーションプロトコルのアイデンティティのいずれかで、アイデンティティの競合が発生している場合、システムは、競合が解決するまで両方のアイデンティティに対して脆弱性を表示します。

NetFlowデータからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクトレベル1：赤）インパクトレベルを割り当てることができません。このような場合は、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を手動で設定します。

サーバーのベンダーおよびバージョンの情報は、ほとんどの場合はトライフィックに含まれていません。デフォルトでは、システムはこのようなトライフィックの送信側および受信側に対して、関連付けられている脆弱性をマップしません。ただし、ベンダーまたはバージョンの情報を持たない特定のアプリケーションプロトコルに対して脆弱性をマップするよう、システムを設定することができます。

ホストの入力機能を使用して、ネットワーク上のホストにサードパーティの脆弱性情報を追加すると、追加の [脆弱性 (Vulnerabilities)] セクションが表示されます。たとえばQualysGuard

Scanner から脆弱性をインポートすると、ホスト プロファイルには [QualysGuard 脆弱性 (QualysGuard Vulnerabilities)] セクションが含まれます。サードパーティの脆弱性の場合は、ホスト プロファイルの対応する [脆弱性 (Vulnerabilities)] セクションの情報は、ホストの入力機能を使用して脆弱性データをインポートしたときに提供した情報に制限されます。

サードパーティの脆弱性をオペレーティング システムおよびアプリケーション プロトコルと関連付けることはできますが、クライアントに関連付けることはできません。サードパーティの脆弱性のインポートについては、『Firepower システムホスト入力 API ガイド』を参照してください。

次に、ホスト プロファイルの [脆弱性 (Vulnerabilities)] セクションのカラムについて説明します。

名前

脆弱性の名前。

[リモート (Remote)]

脆弱性がリモートで不正利用される可能性があるかどうかを示します。この列が空白の場合、脆弱性の定義にはこの情報は含まれていません。

コンポーネント

脆弱性に関連付けられているオペレーティング システム、アプリケーション プロトコル、またはクライアントの名前。

ポート

ポート番号（脆弱性が、特定のポート上で実行されているアプリケーション プロトコルに関連付けられている場合）。

関連トピック

[脆弱性データのフィールド](#)

[脆弱性の非アクティブ化](#)

脆弱性に対するパッチのダウンロード

ネットワーク上のホストで検出された脆弱性を軽減するためのパッチをダウンロードできます。

手順

ステップ1 パッチをダウンロードするホストのホスト プロファイルにアクセスします。

ステップ2 [脆弱性 (Vulnerabilities)] セクションを展開します。

ステップ3 パッチを適用する脆弱性の名前をクリックします。

個々のホストに関する脆弱性の非アクティブ化

ステップ4 [修正 (Fixes)] セクションを展開して、脆弱性に対するパッチの一覧を表示します。

ステップ5 ダウンロードするパッチの隣の [ダウンロード (Download)] をクリックします。

ステップ6 パッチをダウンロードして、影響を受けるシステムに適用します。

個々のホストに関する脆弱性の非アクティブ化

ホストの脆弱性エディタを使用して、ホストごとに脆弱性を非アクティブにすることができます。ホストの脆弱性を非アクティブにしても、そのホストの影響の相関に対して脆弱性は使用されますが、影響レベルは自動的に 1 レベル減少します。

手順

ステップ1 ホストプロファイルの [脆弱性 (Vulnerabilities)] セクションに移動します。

ステップ2 [脆弱性の編集 (Edit Vulnerabilities)] をクリックします。

ステップ3 [有効な脆弱性 (Valid Vulnerabilities)] リストから脆弱性を選択し、下矢印をクリックして [無効な脆弱性 (Invalid Vulnerabilities)] リストに移動します。

ヒント

隣接している複数の脆弱性を選択するには、クリックおよびドラッグを使用します。脆弱性をダブルクリックして、リスト間を移動することもできます。

ステップ4 [保存 (Save)] をクリックします。

次のタスク

- 必要に応じて、ホストの脆弱性を [無効な脆弱性 (Invalid Vulnerabilities)] リストから [有効な脆弱性 (Valid Vulnerabilities)] リストに移動して、脆弱性をアクティブ化します。

関連トピック

[個々の脆弱性の非アクティブ化](#) (30 ページ)

[複数の脆弱性の非アクティブ化](#)

個々の脆弱性の非アクティブ化

ホストプロファイルで脆弱性を非アクティブ化すると、ネットワークマップにあるすべてのホストに対して脆弱性が非アクティブ化されます。ただし、いつでもその脆弱性を再アクティブ化することができます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフドメインでは、脆弱性が先祖ドメインで

アクティブ化された場合、リーフ ドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

手順

ステップ1 次のようにして、脆弱性の詳細にアクセスします。

- 影響を受けるホストプロファイルで、[脆弱性 (Vulnerabilities)] セクションを展開し、有効または無効にする脆弱性の名前をクリックします。
- 事前定義されたワークフローで、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [脆弱性 (Vulnerabilities)] を選択し、有効または無効にする脆弱性の横にある [表示 (View)] (○) をクリックします。

ステップ2 [影響を受ける条件 (Impact Qualification)] ドロップダウンリストから [無効 (Disabled)] を選択します。

コントロールが淡色表示されている場合、設定は先祖 ドメインに属しており、設定を変更する権限がありません。

ステップ3 ネットワークマップ上のすべてのホストに対して、[影響を受ける条件 (Impact Qualification)] の値を変更することを確認します。

ステップ4 [完了 (Done)] をクリックします。

次のタスク

- オプションで、上記の手順を実行中に、[影響を受ける条件 (Impact Qualification)] ドロップダウンリストから [有効 (Enabled)] を選択することによって、脆弱性をアクティブにします。

関連トピック

[個々のホストに関する脆弱性の非アクティブ化](#) (30 ページ)

[複数の脆弱性の非アクティブ化](#)

[オペレーティングシステムのアイデンティティの競合](#) (11 ページ)

ホスト プロファイルのスキャン結果

Nmap を使用してホストをスキャンする場合、または Nmap のスキャンから結果をインポートする場合、これらの結果は、スキャンに含まれているすべてのホストのホストプロファイルに表示されます。

Nmap が、ホストのオペレーティングシステムについて、およびオープンでフィルタリングされていないポート上で稼動している任意のサーバーについて収集した情報が、ホストプロファイルの [オペレーティング システム (Operating System)] と [サーバー (Servers)] セクション

ホストプロファイルからのホストのスキャン

にそれぞれ追加されます。また、Nmap は、そのホストのスキャン結果のリストを [スキャン結果 (Scan Results)] セクションに追加します。プロファイルに [スキャン結果 (Scan Results)] セクションが表示されるのは、スキャンでホスト上のオープンポートが検出された場合のみであることに注意してください。

各結果には、情報のソース、スキャンしたポートの番号とタイプ、ポート上で稼動しているサーバの名前、Nmap で検出された任意の追加情報（ポートの状態やサーバのベンダー名など）が示されます。UDP ポートをスキャンする場合、そのポートで検出されたサーバーは [スキャン結果 (Scan Results)] セクションにのみ表示されます。

ホストプロファイルから Nmap スキャンを実行できることに注意してください。

ホストプロファイルからのホストのスキャン

ホストプロファイルから、ホストに対して Nmap スキャンを実行できます。スキャンが完了すると、ホストプロファイルでそのホストのサーバーおよびオペレーティングシステムの情報が更新されます。追加のスキャン結果は、すべてホストプロファイルの [スキャン結果 (Scan Results)] セクションに追加されます。



注意 Nmap 提供のサーバおよびオペレーティングシステムのデータは、別の Nmap スキャンを実行するか、より優先度の高いホスト入力で上書きするまでスタティックなままになります。Nmap を使用したホストのスキャンを計画している場合は、定期的にスキャンをスケジュールします。

始める前に

- Nmap スキャンインスタンスを追加します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Host Identity Sources*」の章を参照してください。

手順

ステップ1 ホストプロファイルで、[ホストのスキャン (Scan Host)] をクリックします。

ステップ2 ホストのスキャンに使用するスキャン修復の横にある [スキャン (Scan)] をクリックします。

システムによってホストがスキャンされ、ホストプロファイルに結果が追加されます。

関連トピック

[Nmap スキャンの自動化](#)

ホストプロファイルの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
VRFを使用する場合の制限事項	6.6	任意 (Any)	<p>仮想ルーティングおよび転送が環境内で使用されている場合、VRFに重複するネットワークスペースが含まれている可能性があるため、単一の IP アドレスが複数のホストを表すことがあります。</p> <p>サポート対象プラットフォーム： Firewall Management Center</p>

ホストプロファイルの履歴

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。