ホスト ID ソース

次のトピックでは、ホスト ID ソースについて説明します。

概要：ホストのデータ収集

Firepower システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の固有データを設定された定義と比較して（フィンガープリントと呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で実行中のオペレーティング システム
- ホスト上のアプリケーションとそのアプリケーションに関連付けられているユーザ

システムがホストのオペレーティング システムを特定できない場合、カスタムのクライアントまたはサーバのフィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシステムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。

（注） システムはモニタ対象のネットワーク トラフィックからだけでなく、エクスポートされた NetFlow レコードからもホスト データを収集することができ、また Nmap スキャンやホスト入力機能を使用してアクティブにホスト データを追加することもできます。

システムが検出できるホストオペレーティングシステムの判別

システムがどのオペレーティング システムのフィンガープリントを作成できるかを確認するには、カスタム OS フィンガープリントの作成プロセス中に表示される、使用可能なフィンガープリントの一覧を表示します。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションにあるドロップダウン リスト内のオプションのリストを表示します。これらのオプションが、システムがフィンガープリントを作成できるオペレーティング システムになります。

次のタスク

必要に応じて、ホスト オペレーティング システムの識別 （2 ページ）を参照してください。

ホスト オペレーティング システムの識別

システムがホストのオペレーティング システムを正しく識別しない場合（たとえばホスト プロファイル「不明」を示したり間違って識別したりする場合）には、下記の方法を試してください。

手順

次のいずれかの方法を試します。

- ネットワーク検出アイデンティティ競合設定を確認します。
- ホストのカスタム フィンガープリントを作成します。

- ホストに対して Nmap スキャンを実行します。
- ホスト入力機能を使用して、ネットワーク マップにデータをインポートします。
- オペレーティング システム情報を手動で入力します。

カスタムフィンガープリント

Firepower システムには、検出された各ホストのオペレーティング システムを識別するためにシステムが使用するオペレーティング システムのフィンガープリントが含まれます。しかし、オペレーティング システムに一致するフィンガープリントがないため、システムがホスト オペレーティング システムを識別できない、または誤って識別することがあります。この問題を解決するために、不明または誤認されたオペレーティング システムに固有のオペレーティング システム特性のパターンを提供するカスタム フィンガープリントを作成し、識別用のオペレーティング システムの名前を提供することができます。

システムはオペレーティング システムのフィンガープリントから各ホストの脆弱性リストを取得するため、システムがホストのオペレーティング システムを照合できない場合、ホストの脆弱性を識別することはできません。たとえば、システムが Microsoft Windows を実行中のホストを検出した場合、そのシステムには保存された Microsoft Windows の脆弱性リストが存在します。このリストは、検出した Windows オペレーティング システムに基づいて、そのホストのホスト プロファイルに追加されます。

たとえば、ネットワーク上に Microsoft Windows の新しいベータ バージョンを実行中の複数のデバイスがある場合、システムはそのオペレーティング システムを識別できず、脆弱性をそれらのホストにマッピングすることもできません。しかし、システムに Microsoft Windows に関する脆弱性のリストがあるならば、同じオペレーティング システムを実行中の他のホストを識別できるように、いずれか 1 台のホストに対してカスタム フィンガープリントを作成できます。フィンガープリントに Microsoft Windows の脆弱性リストのマッピングを含め、フィンガープリントに一致する各ホストとそのリストを関連付けることができます。

カスタム フィンガープリントを作成すると Firepower Management Center は、同じオペレーティング システムを実行中のすべてのホストに関するそのフィンガープリントに関連付けられた脆弱性のセットをリストします。ユーザが作成したカスタム フィンガープリントに脆弱性マッピングが 1 つも存在しない場合、システムはフィンガープリントを使用して、フィンガープリントで提供するカスタム オペレーティング システムの情報を割り当てます。以前に検出されたホストからの新しいトラフィックが確認されると、システムはそのホストを新しいフィンガープリント情報で更新します。さらに、そのオペレーティング システムを実行する新しいホストの最初の検出時に、新しいフィンガープリントを使用して識別します。

カスタム フィンガープリントを作成する前に、ホストが正しく識別されない理由を特定して、カスタム フィンガープリントが実行可能なソリューションであるかどうかを判断する必要があります。

以下の 2 種類のフィンガープリントを作成できます。

- クライアントのフィンガープリント。ネットワーク上の別のホストで実行中の TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。
- サーバのフィンガープリント。実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。

（注） クライアントとサーバの両方のフィンガープリントが同じホストに一致する場合、クライアントのフィンガープリントが使用されます。

フィンガープリントを作成した後、システムがフィンガープリントをホストに関連付けるには、その前に、フィンガープリントを有効化する必要があります。

関連トピック

クライアント用のカスタム フィンガープリントの作成 （8 ページ）
サーバ用のカスタム フィンガープリントの作成 （11 ページ）

フィンガープリントの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントを作成してアクティブにした後、フィンガープリントを編集して変更を加えたり、脆弱性マッピングを追加したりできます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。システムがフィンガープリントを作成するデータを待機している場合、フィンガープリントが作成されるまで 10 秒ごとに自動的に更新されます。

ステップ 3 カスタムのフィンガープリントを管理します。

- アクティブ化/非アクティブ化：フィンガープリントをアクティブ化または非アクティブ化します。詳細については、フィンガープリントのアクティブおよび非アクティブの設定（5 ページ）を参照してください。

- 作成：フィンガープリントを作成します。詳細については、クライアント用のカスタム フィンガープリントの作成 （8 ページ）およびサーバ用のカスタム フィンガープリントの作成 （11 ページ）を参照してください。
- 編集：フィンガープリントを編集します。詳細については、アクティブなフィンガープリントの編集 （6 ページ）および非アクティブなフィンガープリントの編集 （7 ページ）を参照してください。
- 削除：削除するフィンガープリントの横にある削除アイコン（）をクリックして、確認のために [OK] をクリックします。削除できるのは、非アクティブ化したフィンガープリントのみです。

フィンガープリントのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

ホストを識別するためにシステムがカスタム フィンガープリントを使用できるようにするには、その前に、カスタム フィンガープリントをアクティブにする必要があります。新しいフィンガープリントがアクティブにされた後は、以前に検出したホストを再識別し、新しいホストを検出するために使用されます。

フィンガープリントの使用を停止する場合は、それを非アクティブにすることができます。フィンガープリントを非アクティブにすると、フィンガープリントは使用できなくなりますが、システム上で維持できます。フィンガープリントを非アクティブにすると、オペレーティング システムは、フィンガープリントを使用しているホストに対して不明としてマークされます。ホストが再度検出され、別のアクティブなフィンガープリントに一致すると、ホストはそのアクティブなフィンガープリントによって識別されます。

フィンガープリントを削除すると、システムから完全に削除されます。フィンガープリントを非アクティブにした後に削除できます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするフィンガープリントの横にあるスライダをクリックします。

（注） アクティブ化オプションは、作成したフィンガープリントが有効である場合に限り使用できます。スライダが使用できない場合、フィンガープリントを再作成してください。

アクティブなフィンガープリントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントがアクティブである場合、フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

フィンガープリントの名前、説明、オペレーティング システムのカスタム表示の変更、および追加の脆弱性のフィンガープリントへのマッピングを行えます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム オペレーティング システム（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（  ）をクリックします。

ステップ 4 必要に応じて、フィンガープリントの名前、説明、およびカスタム OS 表示を変更します。

ステップ 5 脆弱性マッピングを削除する場合は、ページの [事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] セクションのマッピングの横にある [削除（Delete）] をクリックします。

ステップ 6 脆弱性マッピングにその他のオペレーティング システムを追加する場合は、[製品（Product）] を選択し（該当する場合は [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および[拡張（Extension）] も選択します）、[OS 定義の追加（Add OS Definition）] をクリックします。

脆弱性マッピングが、[事前定義された OS 製品マップ（Pre-Defined OS Product Maps）] リストに追加されます。

ステップ 7 [保存（Save）] をクリックします。

非アクティブなフィンガープリントの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

フィンガープリントが非アクティブである場合は、フィンガープリントのすべての要素を変更し、それらを Firepower Management Center に再送信できます。これには、フィンガープリントのタイプ、ターゲットの IP アドレスとポート、脆弱性マッピングなど、フィンガープリントの作成時に指定したすべてのプロパティが含まれます。非アクティブのフィンガープリントを編集および送信すると、システムに再送信されます。また、それがクライアントのフィンガープリントである場合、アクティブにする前に、アプライアンスにトラフィックを再送信する必要があります。非アクティブのフィンガープリントに対して選択できる脆弱性マッピングは 1 つだけであることに注意してください。フィンガープリントをアクティブにした後、追加のオペレーティング システムおよびバージョンを脆弱性リストにマッピングすることができます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 編集するフィンガープリントの横にある編集アイコン（）をクリックします。

ステップ 4 必要に応じてフィンガープリントを変更します。

- クライアントのフィンガープリントを変更している場合は、クライアント用のカスタム フィンガープリントの作成 （8 ページ）を参照してください。
- サーバのフィンガープリントを変更している場合は、サーバ用のカスタム フィンガープリントの作成 （11 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- クライアントのフィンガープリントを変更した場合は、ホストからフィンガープリントを収集しているアプライアンスにトラフィックを必ず送信してください。

クライアント用のカスタム フィンガープリントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

クライアントのフィンガープリントは、クライアントがネットワーク上の別のホストで実行する TCP アプリケーションに接続されている場合、ホストが送信する SYN パケットに基づいてオペレーティング システムを識別します。

Firepower Management Center が監視対象ホストと直接通信することがない場合は、クライアントのフィンガープリントのプロパティを指定するときに、Management Center によって管理され、フィンガープリントを作成するホストに最も近いデバイスを指定することができます。

フィンガープリント作成プロセスを開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用する Firepower Management Center またはデバイスの間のネットワーク ホップの数。（Cisco では、ホストが接続されている同じサブネットに Firepower Management Center またはデバイスを直接接続することを強く推奨します）。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（Firepower Management Center またはデバイス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- クライアント トラフィックを生成するためのホストへのアクセス。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] ドロップダウンリストから、フィンガープリントを収集するために使用する Firepower Management Center またはデバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、[クライアント（Client）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意 これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意 Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合（またはフィンガープリントを作成するホストが [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションに存在しない場合）、[カスタム OS 表示の使用（Use Custom OS Display）] を選択して、次に示すように表示する値を指定します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 12 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに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。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションで [ベンダー（Vendor）] と [製品（Product）] の値名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、[ベンダー（Vendor）] および [製品（Product）] の値のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

たとえば、カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、メジャー バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 13 [作成（Create）] をクリックします。

ステータスは一時的に [新規（New）] になってから、[保留中（Pending）] に切り替わります。フィンガープリントのトラフィックが確認されるまで、このステータスが維持されます。トラフィックが確認されると、[使用可（Ready）] に切り替わります。

当該のホストからデータを受信するまで、[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新されます。

ステップ 14 ターゲット IP アドレスとして指定した IP アドレスを使用して、フィンガープリントを作成しようとしているホストにアクセスし、アプライアンスへの TCP 接続を開始します。

正確なフィンガープリントを作成するためには、トラフィックがフィンガープリントを収集するアプライアンスで認識される**必要**があります。スイッチを経由して接続している場合は、アプライアンス以外のシステムへのトラフィックはシステムによって認識されない場合があります。

例：

フィンガープリントを作成しようとしているホストから Firepower Management Center の Web インターフェイスにアクセスするか、ホストから SSH で Management Center にアクセスします。SSH を使用する場合は、次に示すコマンドを使用します。このコマンドの localIPv6address は、現在ホストに割り当てられているステップ 7 で指定した IPv6 アドレスです。DCmanagementIPv6address は、Management Center の管理 IPv6 アドレスです。[カスタム フィンガープリント（Custom Fingerprint）] ページが [使用可（Ready）] ステータスでリロードされるようになります。

```
ssh -b localIPv6address DCmanagementIPv6address
```

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定 （5 ページ） で説明するように、フィンガープリントをアクティブにします。

サーバ用のカスタム フィンガープリントの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Discovery Admin

サーバのフィンガープリントは、実行中の TCP アプリケーションへの着信接続に応答するためにホストが使用する SYN-ACK パケットに基づいてオペレーティング システムを識別します。開始する前に、フィンガープリントを作成するホストに関する次の情報を取得します。

- ホストとフィンガープリントを取得するために使用するアプライアンスの間のネットワーク ホップの数。Cisco では、ホストが接続されている同じサブネットにアプライアンスの使用されていないインターフェイスを直接接続することを強く推奨します。
- ホストが存在するネットワークに接続されているネットワーク インターフェイス（アプライアンス上）。
- ホストの実際のオペレーティング システム ベンダー、製品、バージョン。
- 現在未使用の、ホストが存在するネットワーク上で許可されている IP アドレス。

ヒント Firepower Management Center が監視対象ホストと直接通信することがない場合は、サーバのフィンガープリントのプロパティを指定するときに、フィンガープリントを作成するホストに最も近い管理対象デバイスを指定することができます。

手順

ステップ 1 **[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）]**を選択します。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 2 [カスタム OS（Custom Operating Systems）] をクリックします。

ステップ 3 [カスタム フィンガープリントの作成（Create Custom Fingerprint）] をクリックします。

ステップ 4 [デバイス（Device）] リストから、フィンガープリントを収集するために使用する Firepower Management Center または管理対象デバイスを選択します。

ステップ 5 [フィンガープリント名（Fingerprint Name）] を入力します。

ステップ 6 [フィンガープリントの説明（Fingerprint Description）] を入力します。

ステップ 7 [フィンガープリント タイプ（Fingerprint Type）] リストから、サーバのフィンガープリント作成オプションを表示する [サーバ（Server）] を選択します。

ステップ 8 [ターゲット IP アドレス（Target IP Address）] フィールドで、フィンガープリントを作成するホストの IP アドレスを入力します。

フィンガープリントは、ホストに他の IP アドレスが存在していても、ユーザが指定したホスト IP アドレスから送受信されるトラフィックにのみ基づくことに注意してください。

注意 Firepower システムのバージョン 5.2 以降を実行するアプライアンスでのみ IPv6 フィンガープリントをキャプチャできます。

ステップ 9 [ターゲット距離（Target Distance）] フィールドで、前の手順で選択したフィンガープリントを収集するデバイスとホストの間のネットワーク ホップ数を入力します。

注意 これは、ホストへの実際の物理ネットワーク ホップ数である必要があります。システムによって検出されるホップ数と同じになる場合も、同じにならない場合もあります。

ステップ 10 [インターフェイス（Interface）] リストから、ホストが存在するネットワーク セグメントに接続されているネットワーク インターフェイスを選択します。

注意 Cisco では、いくつかの理由でフィンガープリントの作成に管理対象デバイスのセンシング インターフェイスを使用**しない**ことを推奨します。まず、フィンガープリントは、センシング インターフェイスが SPAN ポート上にあると機能しません。また、デバイスでセンシング インターフェイスを使用する場合、デバイスはフィンガープリントを収集している間、ネットワークの監視を停止します。ただし、フィンガープリントの収集を実行するために、管理インターフェイスまたはその他の使用可能なネットワーク インターフェイスを使用できます。どのインターフェイスがデバイスのセンシング インターフェイスであるかがわからない場合は、フィンガープリントの作成に使用している特定のモデルのインストレーション ガイドを参照してください。

ステップ 11 [アクティブ ポートの取得（Get Active Ports）] をクリックします。

ステップ 12 [サーバ ポート（Server Port）] フィールドに、フィンガープリントを収集するように選択したデバイスが通信を開始するポートを入力します。または、[アクティブ ポートの取得（Get Active Ports）] ドロップダウンリストからポートを選択します。

ホストでオープンしていると判明しているすべてのサーバ ポートを使用できます（たとえば、ホストで Web サーバを実行している場合は 80）。

ステップ 13 [送信元 IP アドレス（Source IP Address）] フィールドで、ホストとの通信を試行するために使用する IP アドレスを入力します。

ネットワークでの使用が許可されていて、現在未使用の送信元 IP アドレス（たとえば、現在使用されていない DHCP プール アドレス）を使用する必要があります。これにより、フィンガープリントの作成中に、別のホストを一時的にオフラインにすることを防ぎます。

フィンガープリントを作成している間は、その IP アドレスをネットワーク検出ポリシーでモニタリングから除外する必要があります。そうしていないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。

ステップ 14 [送信元サブネット マスク（Source Subnet Mask）] フィールドには、ユーザが使用している IP アドレスのサブネット マスクを入力します。

ステップ 15 [送信元ゲートウェイ（Source Gateway）] フィールドが表示されたら、ホストへのルートを確立するために使用するデフォルトのゲートウェイ IP アドレスを入力します。

ステップ 16 フィンガープリントを作成したホストのホスト プロファイルのカスタム情報を表示する場合、または使用するフィンガープリントの名前が [OS 定義（OS Definition）] セクションに存在しない場合、[カスタム OS 表示（Custom OS Display）] セクションの [カスタム OS 表示の使用（Use Custom OS Display）] を選択します。

以下のように、ホスト プロファイルで表示する値を入力します。

- [ベンダー文字列（Vendor String）] フィールドに、オペレーティング システムのベンダー名を入力します。たとえば、Microsoft Windows のベンダーは「Microsoft」になります。
- [製品文字列（Product String）] フィールドに、オペレーティング システムの製品名を入力します。たとえば、Microsoft Windows 2000 の製品名は「Windows」になります。
- [バージョン文字列（Version String）] フィールドに、オペレーティング システムのバージョン番号を入力します。たとえば、Microsoft Windows 2000 のバージョン番号は「2000」になります。

ステップ 17 [OS 脆弱性マッピング（OS Vulnerability Mappings）] セクションで、脆弱性マッピングに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。

フィンガープリントを使用して一致するホストの脆弱性を識別する場合、またはオペレーティング システムのカスタム表示情報を割り当てない場合、このセクションでベンダーと製品名を指定する必要があります。

オペレーティング システムのすべてのバージョンの脆弱性をマッピングするには、ベンダーおよび製品名のみを指定します。

（注） [メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[リビジョン バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、および [拡張（Extension）] ドロップダウンリストのオプションの中には、選択したオペレーティング システムに該当しないものもあります。また、フィンガープリントを作成するオペレーティング システムに一致するリストに表示される定義がない場合は、それらの値を空のままにすることができます。フィンガープリントで OS の脆弱性マッピングを作成しない場合、システムはそのフィンガープリントを使用して、脆弱性リストをフィンガープリントによって識別されるホストに割り当てることはできないことに注意してください。

例：

カスタム フィンガープリントで Redhat Linux 9 の脆弱性リストを一致するホストに割り当てる場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

例：

Palm OS のすべてのバージョンを追加するには、[ベンダー（Vendor）] リストから [PalmSource, Inc.]、[製品（Product）] リストから [Palm OS] を選択し、その他のすべてのリストはデフォルトの設定のままにします。

ステップ 18 [作成（Create）] をクリックします。
[カスタム フィンガープリント（Custom Fingerprint）] ステータス ページは 10 秒ごとに更新され、[使用可（Ready）] ステータスでリロードされます。

（注） ターゲット システムがフィンガープリント作成プロセス中に応答を停止した場合、ステータスにはメッセージ「エラー：応答がありません（ERROR: No Response）」が示されます。このメッセージが表示された場合は、フィンガープリントを再度送信します。3 ～ 5 分間（時間はターゲット システムによって異なる場合があります）待機して、編集アイコン（  ）をクリックし、[カスタム フィンガープリント（Custom Fingerprint）] ページにアクセスしてから [作成（Create）] をクリックします。

次のタスク

- フィンガープリントのアクティブおよび非アクティブの設定 （5 ページ） で説明するように、フィンガープリントをアクティブにします。

ホスト入力データ

サードパーティからネットワーク マップ データをインポートすることで、ネットワーク マップを増強することができます。また、Web インターフェイスを使用して、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 を変更するか、アプリケーション プロトコル、プロトコル、ホスト属性、クライアントを削除することによって、ホスト入力機能を使用することができます。

システムは複数のソースからのデータを照合して、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行 ID を判別できます。

ネットワーク マップから影響を受けるホストを削除すると、サードパーティの脆弱性を除くすべてのデータは破棄されます。スクリプトまたはインポート ファイルの設定方法の詳細については、『*Firepower System Host Input API Guide*』を参照してください。

影響の関連付けにインポートしたデータを含めるには、データベースのオペレーティング システムおよびアプリケーション定義にデータをマッピングする必要があります。

サードパーティのデータを使用するための要件

ネットワーク上のサードパーティのシステムから検出データをインポートできます。ただし、Firepower の推奨、アダプティブ プロファイルの更新、影響評価などの侵入データおよび検出データを共に使用する機能を有効にするには、対応する定義に対して、可能な限り多くのエレメントをマッピングする必要があります。サードパーティのデータを使用するには、以下の要件を考慮してください：

- サードパーティのシステムにネットワーク アセット上に特定のデータがある場合、ホスト入力機能によりそのデータをインポートできます。しかし、サードパーティが異なる製品名をつける可能性があることから、対応する Cisco 製品の定義に対して、サードパーティベンダー、製品、バージョンをマッピングする必要があります。製品をマッピング後、Firepower Management Center 設定の影響を評価するために脆弱性のマッピングを有効にして、影響相関を可能にします。バージョンまたはベンダーに関係のないアプリケーション プロトコルでは、Firepower Management Center 設定におけるアプリケーション プロトコルの脆弱性をマッピングする必要があります。
- サードパーティからパッチ情報をインポートし、そのパッチで修正されたすべての脆弱性に無効とマークする場合は、サードパーティの修正名をデータベースの修正定義にマッピングする必要があります。修正によって解決された脆弱性はすべて、その修正を加えるホストから排除されます。
- オペレーティング システムやアプリケーション プロトコルの脆弱性をサードパーティからインポートし、これらを影響相関に使用する場合、サードパーティの脆弱性識別文字列をデータベース内の脆弱性にマッピングする必要があります。多くのクライアントは、脆弱性と関連があり、影響評価に使用されますが、サードパーティのクライアントの脆弱性をインポートし、マッピングすることはできない点にご注意ください。脆弱性のマッピング後、Firepower Management Center 設定の影響評価のためにサードパーティの脆弱性のマッピングを有効にします。ベンダー情報やバージョン情報のないアプリケーションプロトコルを脆弱性にマッピングするには、管理ユーザは、Firepower Management Center 設定のアプリケーションの脆弱性もマッピングする必要があります。
- アプリケーションデータをインポートし、そのデータを影響相関に使用する場合、各アプリケーションプロトコルのベンダー文字列を対応する Cisco アプリケーション プロトコルの定義にマッピングする必要があります。

関連トピック

サードパーティの製品のマッピング （16 ページ）
サード パーティ製品の修正のマッピング （18 ページ）
サードパーティの脆弱性のマッピング （19 ページ）
サーバの脆弱性のマッピング
カスタム製品マッピングの作成 （21 ページ）

サードパーティ製品のマッピング

ユーザ入力機能を使用して各サードパーティからのデータをネットワークマップに追加する場合、サードパーティで使用するベンダー、製品、およびバージョンの各名前を Cisco 製品定義にマッピングする必要があります。各製品を Cisco の定義にマッピングすると、これらの定義に基づいて脆弱性が割り当てられます。

同様に、パッチ管理製品などのサードパーティからのパッチ情報をインポートする場合、その修正の名前をデータベース内の適切なベンダー、製品、および対応する修正にマッピングする必要があります。

サードパーティの製品のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

サード パーティからデータをインポートする場合、そのデータを使用して脆弱性を指定したり、影響の関連付けを行ったりするために、シスコの製品をサードパーティの名前にマッピングする必要があります。製品をマッピングすることにより、シスコの脆弱性情報をサードパーティ製品の名前に関連付けます。これにより、システムはそのデータを使用して影響の関連付けを行うことができます。

ホスト入力のインポート機能を使用してデータをインポートする場合、AddScanResult 機能を使用して、インポート中にサードパーティ製品をオペレーティングシステムとアプリケーションの脆弱性にマップピングすることもできます。

たとえば、Apache Tomcat をアプリケーションとしてリストしているサード パーティのデータをインポートする場合で、それがバージョン 6 の Apache Tomcat であれば、以下のように設定し、サード パーティのマッピングを追加します。

- ベンダー名を [Apache] に設定します。
- プロダクト名に [Tomcat] 設定します。
- ベンダーのドロップダウン リストから [Apache] を選択します。
- 製品のドロップダウン リストから [Tomcat] を選択します。
- バージョンのドロップダウン リストから [6] を選択します。

このマッピングによって、Apache Tomcat 6 のすべての脆弱性が、Apache Tomcat をアプリケーションとしてリストアップするホストに割り当てられます。

バージョン情報やベンダー情報のないのアプリケーションの場合、Firepower Management Center 構成のアプリケーションタイプで脆弱性をマッピングする必要があります。多くのクライアントには関連付けられた脆弱性があり、クライアントが影響アセスメントに使用されますが、サードパーティのクライアントの脆弱性をインポートしてマッピングすることはできないことに注意してください。

ヒント　すでに別のFirepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、このManagement Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1　**[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2　[ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3　次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、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 4　[マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5　[説明（Description）] を入力します。

ステップ 6　次の 2 つの選択肢があります。

- [作成（Creat）] : サード パーティ製品をマッピングするには、[製品マップの追加（Add Product Map）] をクリックします。
- [編集（Edit）] : 既存のサードパーティの製品のマッピングを編集するには、そのマッピングの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、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 7　サードパーティの製品で使用される [ベンダーの文字列（Vendor String）] を入力します。

ステップ 8　サードパーティの製品で使用される [製品の文字列（Product String）] を入力します。

ステップ 9　サードパーティの製品で使用される [バージョン文字列（Version String）] を入力します。

ステップ 10　製品マッピング セクションで、ベンダーの脆弱性のマッピングに使用するオペレーティング システム、製品、製品バージョンを、以下の項目から選択します。[ベンダー（Vendor）]、[製品（Product）]、[メジャー バージョン（Major Version）]、[マイナー バージョン（Minor Version）]、[改訂バージョン（Revision Version）]、[ビルド（Build）]、[パッチ（Patch）]、[拡張子（Extension）]。

例：

名前がサードパーティの文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性マッピングを使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Red Hat Linux]、バージョンとして [9] を選択します。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

サーバの脆弱性のマッピング

サードパーティ製品の修正のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

修正名をデータベースの特定の修正セットにマッピングする場合、サードパーティのパッチ管理アプリケーションからデータをインポートし、修正を一連のホストに適用することができます。修正名がホストにインポートされると、システムはその修正によって解決されるすべての脆弱性をそのホストに対して無効としてマークします。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- [作成（Creat）] : 新しいマップ セットを作成するには、[製品マップ セットの作成（Create Product Map Set）] をクリックします。
- [編集（Edit）] : 既存のマップ セットを編集するには、そのマップ セットの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、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 4 [マッピング セット名（Mapping Set Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 次の 2 つの選択肢があります。

- 作成：サードパーティ製品をマッピングするには、[修正マップの追加（Add Fix Map）] をクリックします。
- 編集：既存のサードパーティ製品マップを編集するには、その横にある編集アイコン（）をクリックします。代わりに表示アイコン（  ）が表示される場合、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 7 [サードパーティの修正名（Third-Party Fix Name）] フィールドにマッピングする修正の名前を入力します。

ステップ 8 [製品マッピング（Product Mappings）] セクションで、次のフィールドから修正マッピングに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。

- ベンダー
- 製品
- メジャー バージョン（**Major Version**）
- マイナー バージョン（**Minor Version**）
- リビジョン バージョン（**Revision Version**）
- ビルド（**Build**）
- パッチ（**Patch**）
- 内線番号

例：

Red Hat Linux 9 からパッチが適用されるホストにマッピングで修正を割り当てる場合は、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

ステップ 9 [保存（Save）] をクリックして、修正マップを保存します。

サードパーティの脆弱性のマッピング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

サードパーティからの脆弱性情報を VDB に追加するには、インポートしたそれぞれの脆弱性のサードパーティ識別文字列を、既存の SVID、Bugtraq、または SID にマッピングする必要があります。脆弱性のマッピングを作成したら、マッピングはネットワーク マップのホストにインポートされたすべての脆弱性に対して機能し、それらの脆弱性に対する影響の関連付けを可能にします。

サードパーティの脆弱性に対する影響の関連付けを有効にし、関連付けの実行を可能にする必要があります。バージョンレスまたはベンダーレスのアプリケーションの場合、Firepower Management Center の設定でアプリケーション タイプの脆弱性をマッピングする必要もあります。

多くのクライアントには関連付けられた脆弱性があり、クライアントが影響評価に使用されますが、サードパーティのクライアントの脆弱性は影響評価に使用できません。

ヒント すでに別の Firepower Management Center にサードパーティのマッピングを作成している場合、そのマッピングをエクスポートして、この Management Center にインポートすることができます。その後、必要に応じてインポートしたマッピングを編集できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2 [ユーザ サードパーティ マッピング（User Third-Party Mappings）] をクリックします。

ステップ 3 次の 2 つの選択肢があります。

- 作成：新しい脆弱性セットを作成するには、[脆弱性マップセットの作成（Create Vulnerability Map Set）] をクリックします。
- 編集：既存の脆弱性セットを編集するには、脆弱性セットの横にある編集アイコン（  ）をクリックします。代わりに表示アイコン（  ）が表示される場合、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 4 [脆弱性マップの追加（Add Vulnerability Map）] をクリックします。

ステップ 5 [脆弱性 ID（Vulnerability ID）] フィールドに脆弱性のサードパーティ ID を入力します。

ステップ 6 [脆弱性の説明（Vulnerability Description）] を入力します。

ステップ 7 必要に応じて、次の操作を実行します。

- [Snort 脆弱性 ID マッピング（Snort Vulnerability ID Mappings）] フィールドに Snort ID を入力します。
- [SVID マッピング（SVID Mappings）] フィールドに、レガシー脆弱性 ID を入力します。
- [Bugtraq 脆弱性 ID マッピング（Bugtraq Vulnerability ID Mappings）] フィールドに、Bugtraq ID 番号を入力します。

ステップ 8 [追加（Add）] をクリックします。

関連トピック

ネットワーク検出の脆弱性影響評価の有効化
サーバの脆弱性のマッピング

カスタム製品マッピング

製品マッピングを使用して、サードパーティによるサーバ入力が適切なシスコ定義に関連付けられていることを確認できます。製品マッピングを定義し有効化した後、マッピングされたベンダー文字列を持つモニタ対象ホスト上のすべてのサーバまたはクライアントが、カスタム製品マッピングを使用します。したがって、サーバのベンダー、製品、バージョンを明示的に設定する代わりに、特定のベンダー文字列でネットワーク マップのすべてのサーバの脆弱性をマップすることをお勧めします。

カスタム製品マッピングの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

システムが VDB のベンダーおよび製品にサーバをマッピングできない場合は、手動でマッピングを作成できます。カスタム製品マッピングをアクティブにすると、システムは指定されたベンダーおよび製品の脆弱性を、そのベンダー文字列が発生するネットワーク マップのすべてのサーバにマッピングします。

（注） カスタム製品マッピングは、アプリケーション データのソース（Nmap、ホスト入力機能、Firepower システム自体など）に関係なく、アプリケーション プロトコルのすべての発生に適用されます。ただし、ホスト入力機能を使用してインポートしたデータのサードパーティの脆弱性マッピングが、カスタム製品マッピングを介して設定したマッピングと競合する場合、サードパーティの脆弱性マッピングはカスタム製品マッピングをオーバーライドし、入力が発生したときにサードパーティの脆弱性マッピング設定を使用します。

製品マッピング リストを作成し、各リストをアクティブ化/非アクティブ化することによって、複数のマッピングの同時使用を有効にするか、無効にします。マッピングするベンダーを指定すると、そのベンダーによって作成された製品のみを含むように製品リストが更新されます。

カスタム製品マッピングを作成した後で、カスタム製品マッピング リストをアクティブにする必要があります。カスタム製品マッピング リストをアクティブにすると、指定されたベンダー文字列が発生するすべてのサーバが更新されます。ホスト入力機能を介してインポートされるデータでは、このサーバの製品マッピングをすでに明示的に設定していない限り、脆弱性が更新されます。

たとえば、組織が Apache Tomcat Web サーバのバナーの文字列を `Internal Web Server` に変更した場合、ベンダー文字列 `Internal Web Server` をベンダー **Apache** および製品 **Tomcat** にマッピングできます。その後、そのマッピングを含むリストをアクティブにすると、`Internal Web Server` とラベル付けされたサーバが存在するすべてのホストのデータベースに Apache Tomcat の脆弱性が想定されます。

ヒント この機能を使用して、もう 1 つの脆弱性にルールの SID をマッピングすることによって、ローカルの侵入ルールに脆弱性をマッピングすることができます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 [カスタム製品マッピング リストの作成（Create Custom Product Mapping List）] をクリックします。

ステップ 4 [カスタム製品マッピング リスト名（Custom Product Mapping List Name）] を入力します。

ステップ 5 [ベンダー文字列の追加（Add Vendor String）] をクリックします。

ステップ 6 [ベンダー文字列（Vendor String）] フィールドに、選択したベンダーおよび製品値にマッピングする必要があるアプリケーションを識別するベンダー文字列を入力します。

ステップ 7 [ベンダー（Vendor）] ドロップダウン リストから、マッピングするベンダーを選択します。

ステップ 8 [製品（Product）] ドロップダウン リストから、マッピングする製品を選択します。

ステップ 9 [追加（Add）] をクリックして、マッピングしたベンダー文字列をリストに追加します。

ステップ 10 オプションで、さらにベンダー文字列のマッピングをリストに追加するには、必要に応じて手順 4 ～ 8 を繰り返します。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

- カスタム製品マッピング リストをアクティブにします。詳細については、カスタム製品マッピングのアクティブおよび非アクティブの設定 （23 ページ）を参照してください。

カスタム製品マッピング リストの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ベンダー文字列を追加または削除したり、リスト名を変更したりして、既存のカスタム製品マッピング リストを変更できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品マッピング（Custom Product Mappings）] をクリックします。

ステップ 3 編集する製品マッピング リストの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、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 4 カスタム製品マッピングの作成 （21 ページ）の説明に従って、リストを変更します。

ステップ 5 終了したら、[保存（Save）] をクリックします。

カスタム製品マッピングのアクティブおよび非アクティブの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

カスタム製品マッピング リスト全体の使用を一度に有効または無効にすることができます。カスタム製品マッピング リストをアクティブにすると、そのリストの各マッピングが、管理対象デバイスによって検出されたか、またはホスト入力機能を介してインポートされたかに関わらず、指定したベンダー文字列を持つすべてのアプリケーションに適用されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アプリケーション ディテクタ（Application Detectors）]**を選択します。

ステップ 2 [カスタム製品のマッピング（Custom Product Mappings）] をクリックします。

ステップ 3 アクティブまたは非アクティブにするカスタム製品のマッピング リストの横にあるスライダをクリックします。

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。

eStreamer サーバ ストリーミング

Event Streamer（eStreamer）を使用すると、Firepower Management Center または 7000 または 8000 シリーズ デバイスからの数種類のイベント データを、カスタム開発されたクライアント アプリケーションにストリーム配信できます。詳細については、*Firepower eStreamer Integration Guide*を参照してください。

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。アプライアンスのユーザインターフェイスからこれらすべてのタスクを実行できます。設定が保存されると、選択したイベントが、要求時に、eStreamer クライアントに転送されます。

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

表 *1 : eStreamer* サーバで送信可能なイベント タイプ

イベント タイプ（Event Type）	説明	Management Center で使用可能	7000 & 8000 シリーズ デバイスで使用可能
侵入イベント	管理対象デバイスによって生成される侵入イベント	Yes	Yes
侵入イベント パケット データ	侵入イベントに関連付けられたパケット	Yes	Yes
侵入イベント追加データ	HTTP プロキシまたはロードバランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データ	Yes	Yes
検出イベント	検出イベント	Yes	No
相関およびホワイトリスト イベント	相関およびホワイトリスト イベント	Yes	No
インパクト フラグ アラート	Management Center によって生成されたインパクト アラート	Yes	No
ユーザ イベント	ユーザ イベント	Yes	No
マルウェア イベント	マルウェア イベント	Yes	No
ファイル イベント	ファイル イベント	Yes	No
接続イベント	モニタ対象のホストとその他のすべてのホスト間のセッション トラフィックに関する情報	Yes	Yes

eStreamer イベントタイプの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin

eStreamer サーバで送信可能なイベントの [eStreamer イベント設定（eStreamer Event Configuration）] チェックボックス管理。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、*Firepower eStreamer Integration Guide*を参照してください。

マルチドメイン展開では、どのドメインのレベルでも eStreamer のイベント構成を設定できます。ただし、先祖ドメインで特定のイベントタイプが有効になっている場合は、子孫ドメインのそのイベントタイプを無効にすることはできません。

手順

ステップ 1 **[システム（System）] > [統合（Integration）]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [eStreamer イベント設定（eStreamer Event Configuration）] の下で、eStreamer サーバ ストリーミング （23 ページ）の説明に従って要求元のクライアントに転送するイベントタイプの横にあるチェックボックスをオンまたはオフにします。

ステップ 4 [保存（Save）] をクリックします。

eStreamer クライアント通信の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	Management Center 7000 & 8000 シリーズ	任意（Any）	Admin/Discovery Admin

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了した後、クライアントが eStreamer サーバに接続できるように eStreamer サービスを再起動する必要はありません。

マルチドメイン展開では、任意のドメインで eStreamer クライアントを作成できます。認証証明書では、クライアントはクライアント証明書のドメインと子孫ドメインからのみイベントを要求することが許可されます。eStreamer 設定ページには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは取り消す場合は、クライアントが作成されたドメインに切り替えます。

手順

ステップ 1 **[システム（System）] > [統合（Integration）]**を選択します。

ステップ 2 [eStreamer] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ 6 [保存（Save）] をクリックします。
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 クライアントのホスト名の横にあるファイルのダウンロードアイコン（）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。

eStreamer サービスを再起動する必要はありません。アクセスはただちに取り消されます。

ホスト入力クライアントの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	Management Center	任意（Any）	Admin/Discovery Admin

ホスト入力機能を使用すると、別のアプライアンスで実行されているクライアントプログラムから Firepower Management Center のネットワーク マップを更新できます。たとえば、ネットワーク マップからホストを追加または削除したり、ホスト OS およびサービス情報を更新したりできます。詳細については、*Firepower System Host Input API Guide*を参照してください。

リモート クライアントを実行するには、その前に、[ホスト入力クライアント（Host Input Client）] ページから Firepower Management Center のピア データベースにクライアントを追加する必要があります。また、Management Center によって生成された認証証明書をクライアントにコピーする必要もあります。この手順を完了すると、クライアントは Management Center に接続できます。

マルチドメイン展開では、すべてのドメインにクライアントを作成できます。認証証明書を使用すると、クライアントは、クライアント証明書のドメインに関連付けられているリーフ ドメインにネットワーク マップ アップデートを送信できます。先祖ドメインの証明書を作成した

場合（または後で証明書ドメインが子孫ドメインの追加後に先祖ドメインになった場合）、その証明書を使用するクライアントは、*Firepower System Host Input API Guide*で説明するように、すべてのトランザクションのターゲット リーフ ドメインを指定する必要があります。

[ホスト入力クライアント（Host Input Client）] タブには、現在のドメインに関連付けられているクライアントのみが表示されるため、証明書をダウンロードまたは失効させるには、クライアントが作成されたドメインに切り替えます。

手順

ステップ 1 **[システム（System）] > [統合（Integration）]**を選択します。

ステップ 2 [ホスト入力クライアント（Host Input Client）] タブをクリックします。

ステップ 3 [クライアントの作成（Create Client）] をクリックします。

ステップ 4 [ホスト名（Hostname）]フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） DNS 解決を設定していない場合は、IP アドレスを使用します。

ステップ 5 証明書ファイルを暗号化するには、[パスワード（Password）] フィールドにパスワードを入力します。

ステップ 6 [保存（Save）] をクリックします。
ホスト入力サービスは、ホストが Firepower Management Center 上のポート 8307 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。

ステップ 7 証明書ファイルの横にあるファイル ダウンロード アイコン（）をクリックします。

ステップ 8 SSL 認証のためにクライアントが使用するディレクトリに証明書ファイルを保存します。

ステップ 9 クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。

Nmap スキャン

Firepower システムは、ネットワークのトラフィックをパッシブ分析してネットワーク マップを構築します。このパッシブ分析によって取得される情報は、システムの状態によっては不完全なことがよくあります。ただし、ホストをアクティブにスキャンすることで、完全な情報を取得できます。たとえば、オープンポート上で実行中のサーバがホストにあり、システムによるネットワークのモニタリング中にそのサーバがトラフィックを送受信しなかった場合、システムではそのサーバに関する情報をネットワーク マップに追加しません。しかし、アクティブ スキャナを使用して直接そのホストをスキャンすると、サーバの存在を検出できます。

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。

Nmap を使用してホストをスキャンすると、システムは以下のように動作します。

- 前に検出されていないオープン ポート上のサーバを、該当するホストのホスト プロファイルの [サーバ（Servers）] リストに追加します。ホスト プロファイルの [スキャン結果（Scan Results）] セクションには、フィルタ処理されていたり閉じていたりしている TCP ポートやUDPポート上で検出されたサーバがリストされます。デフォルトでは、Nmapは 1660 を超える TCP ポートをスキャンします。

  Nmap スキャンで識別されたサーバがシステムで認識され、対応するサーバ定義がシステムにある場合、システムは Nmap がそのサーバに使用する名前を、対応する Cisco サーバ定義にマップします。

- スキャン結果と 1500 を超える既知のオペレーティング システムのフィンガープリントを比較して、オペレーティング システムを判別し、それぞれにスコアを割り当てます。最高スコアのオペレーティング システムのフィンガープリントが、ホストに割り当てられるオペレーティング システムになります。

  システムはNmapのオペレーティング システム名をCiscoのオペレーティング システム定義にマップします。

- 追加されたサーバおよびオペレーティング システムのホストに脆弱性を割り当てます。

（注）

- ホストがネットワーク マップ内になければ、Nmapは結果をホストプロファイルに追加することはできません。
- ホストがネットワーク マップから削除されると、そのホストに関するNmapスキャン結果が破棄されます。

ヒント　スキャン オプションによっては（ポートスキャンなど）低帯域幅のネットワークに非常に負荷をかけることがあります。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

スキャンに使用される基礎的な Nmap テクノロジーの詳細については、http://insecure.org/ にある Nmap のマニュアルを参照してください。

関連トピック

Nmap スキャンの自動化

Nmap 修復オプション

Nmap修復を作成して、Nmapスキャンの設定を定義します。Nmap修復は、相関ポリシー内で応答として使用したり、オンデマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合

は、定期的なスキャンのスケジュールをセットアップして、Nmapによって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。

次の表に、Firepower システム上で設定できる Nmap 修復オプションを示します。

表 *2 : Nmap* 修復オプション

オプション	説明	対応する Nmap オプション
[スキャンの開始元イベント（Scan Which Address(es) From Event?）]	Nmap スキャンを相関ルールに対する応答として使用する場合、イベント内の送信元ホスト、宛先ホスト、またはその両方のどのアドレスをスキャンするのか制御する次のいずれかのオプションを選択します。 • [送信元アドレスと宛先アドレスのスキャン（Scan Source and Destination Addresses）] は、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンします。 • [送信元アドレスのみのスキャン（Scan Source Address Only）] は、イベントの送信元 IP アドレスによって表されるホストをスキャンします。 • [宛先アドレスのみのスキャン（Scan Destination Address Only）] は、イベントの宛先 IP アドレスによって表されるホストをスキャンします。	該当なし

オプション	説明	対応する Nmap オプション
[スキャン タイプ（Scan Types）]		**TCP Syn**：`-sS` **TCP Connect**：`-sT` **TCP ACK**：`-sA` **TCP Window**：`-sW` **TCP Maimon**：`-sM`

オプション	説明	対応する Nmap オプション
	Nmap がポートをスキャンする方法を選択します。 • [TCP 同期（TCP Syn）] スキャンは、完全な TCP ハンドシェイクを使用せずに数千のポートにただちに接続します。このオプションを使用すると、TCP 接続が開始されますが完了はしていない状態で、admin アカウントが raw パケットアクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードでクイック スキャンできます。ホストが TCP Syn スキャンで送信される Syn パケットを確認応答すると、Nmap は接続をリセットします。 • [TCP 接続（TCP Connect）] スキャンは、connect() システム コールを使用して、ホスト上のオペレーティング システムを介して接続を開きます。TCP Connect スキャンは、Firepower Management Center 上の admin ユーザや管理対象デバイスがホストに対する raw パケット特権を持っていない場合や、IPv6 ネットワークをスキャンしている場合に使用できます。つまり、このオプションは TCP Syn スキャンを使用できない状況で使用します。 • [TCP ACK] スキャンは、ACK パケットを送信して、ポートがフィルタ処理されているかいないかを検査します。 • [TCP ウィンドウ（TCP Window）] スキャンは、TCP ACK スキャンと同じ機能に加えて、ポートが開いているか閉じているかも判別します。 • [TCP Maimon] スキャンは、FIN/ACK プローブを使用して BSD	

オプション	説明	対応する Nmap オプション
	派生システムを識別します。	
[UDP ポートのスキャン（Scan for UDP ports）]	TCP ポートに加えて UDP ポートのスキャンも有効にします。UDP ポートのスキャンには時間がかかることがあるので、クイック スキャンする場合はこのオプションを使用しないように注意してください。	`-sU`
[イベントからのポートの使用（Use Port From Event）]	相関ポリシー内で応答として修復を使用する計画の場合に、修復によるスキャンの対象として、相関応答をトリガーするイベントで指定されたポートのみを有効にします。 • 相関イベント内のポートをスキャンし、Nmap 修復構成中に指定するポートをスキャンしない場合は、[オン（On）] を選択します。相関イベント内のポートをスキャンする場合は、Nmap 修復構成中に指定する IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。 • Nmap 修復構成中に指定するポートのみスキャンするには、[オフ（Off）] を選択します。 Nmap がオペレーティング システムやサーバに関する情報を収集するかどうかも制御できます。新しいサーバに関連付けられたポートをスキャンするには、[イベントからのポートの使用（Use Port From Event）] オプションを有効にします。	該当なし

オプション	説明	対応する Nmap オプション
[レポート検出エンジンからのスキャン（Scan from reporting detection engine）]	ホストを報告した検出エンジンがあるアプライアンスからホストへのスキャンを有効にします。 • レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン（On）] を選択します。 • 修復内で設定されているアプライアンスからスキャンするには、[オフ（Off）] を選択します。	該当なし
[高速ポートスキャン（Fast Port Scan）]	スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内にある `nmap-services` ファイルにリストされている TCP ポートのみに対するスキャンを有効にし、その他のポート設定を無視できるようにします。このオプションと [ポート範囲とスキャンの順序（Port Ranges and Scan Order）] オプションを併用できないことに注意してください。 • スキャン元デバイス上の `/var/sf/nmap/share/nmap/nmap-services` ディレクトリ内の `nmap-services` ファイルにリストされているポートのみスキャンし、その他のポート設定を無視するには、[オン（On）] を選択します。 • すべての TCP ポートをスキャンするには、[オフ（Off）] を選択します。	`-F`
[ポート範囲とスキャンの順序（Port Ranges and Scan Order）]	Nmap ポート仕様シンタックスを使用して、スキャンする特定のポートを設定し、スキャンする順序も設定します。このオプションと [高速ポートスキャン（Fast Port Scan）] オプションを併用できないことに注意してください。	`-p`

オプション	説明	対応する Nmap オプション
[オープン ポートでベンダーとベンダー情報を調査（Probe open ports for vendor and version information）]	サーバベンダーとバージョン情報の検出を有効にします。オープン ポートでサーバベンダーとバージョン情報を調査する場合、Nmap はサーバの識別に使用するサーバデータを取得します。次に、シスコのサーバ データをそのサーバに置き換えます。 • ホスト上のオープン ポートでサーバ情報をスキャンして、サーバベンダーとバージョンを識別するには、[オン（On）] を選択します。 • ホストのシスコのサーバ情報を使用して続行するには、[オフ（Off）] を選択します。	`-sV`
[サービス バージョンの強度（Service Version Intensity）]	サービス バージョンに対する Nmap プローブの強度を選択します。 • 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。 • 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。	`--version-intensity` <intensity>

オプション	説明	対応する Nmap オプション
[オペレーティング システムの検出（Detect Operating System）]	ホストのオペレーティング システム情報の検出を有効にします。 ホストでのオペレーティング システムの検出を設定した場合、Nmap はホストをスキャンし、その結果を使用してオペレーティング システムごとに評価を作成します。この評価は、ホスト上でそのオペレーティング システムが実行されている可能性を反映します。 • ホストに対してオペレーティング システムを識別する情報をスキャンするには、[オン（On）] を選択します。 • ホストに関するシスコのオペレーティング システム情報を使い続ける場合は、[オフ（Off）] を選択します。	`-o`
[すべてのホストをオンラインとして処理（Treat All Hosts As Online）]	ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを有効にします。このオプションを有効にすると、Nmap は [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリポート リスト（Host Discovery Port List）] の設定を無視するので注意してください。 • ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[オン（On）] を選択します。 • [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[オフ（Off）] を選択します。	`-PN`

オプション	説明	対応する Nmap オプション
[ホスト ディスカバリ方式（Host Discovery Method）]		**TCP SYN**：`-PS` **TCP ACK**：`-PA` **UDP**：`-PU`

オプション	説明	対応する Nmap オプション
	ホストディスカバリを、ターゲット範囲内のすべてのホストに対して実行するか、[ホストディスカバリ ポート リスト（Host Discovery Port List）] にリストされているポートを経由して実行するか、または、ポートがリストされていない場合にそのホストディスカバリ方式のデフォルトポートを経由するかを選択します。 ここで、[すべてのホストをオンラインとして処理（Treat All Hosts As Online）] も有効にすると、[ホストディスカバリ方式（Host Discovery Method）] オプションは無効になり、ホストディスカバリが実行されないことに注意してください。 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。 • [TCP SYN] オプションは、SYN フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP SYN はポート 80 をスキャンします。TCP SYN スキャンは、ステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。 • [TCP ACK] オプションは、ACK フラグが設定された空の TCP パケットを送信し、応答を受信するとホストが利用可能であると認識します。デフォルトでは TCP ACK もポート 80 をスキャンします。TCP ACK スキャンは、ステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。	

オプション	説明	対応する Nmap オプション
	• [UDP] オプションは、UDP パケットを送信し、クローズポートからポート到達不能応答が戻されるとホストが利用可能であると想定します。デフォルトではUDPはポート 40125 をスキャンします。	
[ホスト ディスカバリ ポート リスト（Host Discovery Port List）]	ホストディスカバリの実行時にスキャンするポートを、カスタマイズしたカンマ区切りリストで指定します。	ホストディスカバリ方式に応じたポート リスト
[デフォルト NSE スクリプト（Default NSE Scripts）]	ホストディスカバリを行い、サーバ、オペレーティングシステム、脆弱性を検出する Nmap スクリプトのデフォルトセットを実行できるようにします。デフォルトスクリプトのリストについては、https://nmap.org/nsedoc/categories/default.html を参照してください。 • Nmap スクリプトのデフォルトセットを実行するには、[オン（On）] を選択します。 • Nmap スクリプトのデフォルトセットを省略するには、[オフ（Off）] を選択します。	`-sC`
[タイミング テンプレート（Timing Template）]	スキャンプロセスのタイミングを選択します。選択する数値が大きいほど、スキャンは高速になり包括的ではなくなります。	**0**：`T0`（paranoid） **1**：`T1`（sneaky） **2**：`T2`（polite） **3**：`T3`（normal） **4**：`T4`（aggressive） **5**：`T5`（insane）

Nmap スキャンのガイドライン

アクティブ スキャンにより重要な情報が得られることがありますが、Nmap などのツールを多用すると、ネットワーク リソースに負荷がかかり、重要なホストがクラッシュすることさえあります。アクティブ スキャナを使用する際には、以下のガイドラインに従ってスキャン戦略を作成し、スキャンする必要があるホストとポートのみスキャンするようにしてください。

適切なスキャン ターゲットの選択

Nmap を設定する際に、スキャン対象のホストを識別するスキャン ターゲットを作成できます。スキャン ターゲットには 1 つの IP アドレス、IP アドレスの CIDR ブロックまたはオクテット範囲、IP アドレス範囲、スキャンする IP アドレスまたは範囲のリスト、および 1 つ以上のホスト上のポートが含まれます。

次の方法でターゲットを指定できます。

- IPv6 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）
- IPv4 ホストの場合：
  - 厳密な IP アドレス（`192.168.1.101` など）またはカンマかスペースで区切った IP アドレスのリスト
  - CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストをスキャンします）
  - オクテットの範囲アドレッシングを使用した IP アドレス範囲（たとえば、`192.168.0-255.1-254` は、192.168.x.x の範囲内の末尾が .0 と .255 以外のすべてのアドレスをスキャンします）
  - ハイフンを使用した IP アドレス範囲（たとえば、`192.168.1.1 - 192.168.1.5` は、両端を含めて 192.168.1.1 から 192.168.1.5 の間の 6 つのホストをスキャンします）
  - カンマかスペースで区切ったアドレスか範囲のリスト（たとえば、`192.168.1.0/24, 194.168.1.0/24` は、両端を含めて 192.168.1.1 から 192.168.1.254 の間の 254 個のホストと、両端を含めて 194.168.1.1 から 194.168.1.254 の間の 254 個のホストをスキャンします）

理想的な Nmap スキャンのスキャン ターゲットには、システムで識別できないオペレーティング システムがあるホスト、識別されていないサーバがあるホスト、最近ネットワーク上で検出されたホストが含まれます。ネットワーク マップ内にないホストに関する Nmap 結果は、ネットワーク マップに追加できないことに注意してください。

⚠

注意

- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。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。
- ホストがネットワーク マップから削除されると、Nmap スキャン結果が破棄されます。
- ターゲットをスキャンする権限を持っていることを確認してください。Nmap を使用して自分や自社に属さないホストをスキャンすると違法になる場合があります。

スキャン対象にする適切なポートの選択

設定するスキャンターゲットごとに、スキャン対象のポートを選択できます。各ターゲット上でスキャンする必要があるポートのセットを正確に識別するため、個々のポート番号、ポート範囲、または一連のポート番号やポート範囲を指定できます。

デフォルトでは、Nmap は 1 から 1024 までの TCP ポートをスキャンします。相関ポリシー内で応答として修復を使用する計画の場合は、相関応答をトリガーするイベントで指定されたポートのみを修復でスキャンできます。オンデマンドまたはスケジュール済みタスクとして修復を実行する場合、または Use Port From Event を使用しない場合は、その他のポート オプションを使用して、スキャンするポートを決定できます。`nmap-services` ファイルにリストされている TCP ポートのみスキャンし、その他のポート設定を無視するよう選択できます。TCP ポートの他に UDP ポートもスキャンできます。UDP ポートに対するスキャンには時間がかかることがあるので、すばやくスキャンする場合はこのオプションを使用しないように注意してください。スキャン対象として特定のポートかポート範囲を選択するには、Nmap ポート仕様シンタックスを使用してポートを識別します。

ホスト ディスカバリ オプションの設定

ホストに対してポート スキャンを始める前にホスト ディスカバリを実行するかどうかを決めるか、またはスキャンを計画しているすべてのホストがオンラインであると想定できます。すべてのホストをオンラインとして扱わないことを選択した場合、使用するホストディスカバリ方式を選択でき、必要に応じて、ホストディスカバリ時のスキャン対象ポートのリストをカスタマイズできます。ホストディスカバリ時には、リストされているポートでオペレーティング システムやサーバの情報は調査されません。特定のポートを経由する応答を使用して、ホストがアクティブで使用可能かどうかのみを判別します。ホストディスカバリを実行して、ホストが利用可能でなかった場合には、そのホスト上のポートは Nmap でスキャンされません。

関連トピック

Firepower システムの IP アドレス表記法
Nmap スキャンの自動化

例：Nmap を使用した不明なオペレーティング システムの解決

この例では、不明なオペレーティング システムを解決するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （43 ページ）を参照してください。

システムでネットワーク上のホストのオペレーティング システムを判別できない場合、Nmap を使用してホストをアクティブ スキャンできます。Nmap は、スキャンから得られた情報を利用して、使用されている可能性のあるオペレーティング システムを評価します。次に、最高の評価のオペレーティング システムを、ホストのオペレーティング システムを識別したものとして使用します。

Nmap を使用して新しいホストにオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するシステムによるそのデータのモニタリングは非アクティブになります。Nmap を使用してホスト検出を実行し、システムにより不明なオペレーティング システムがあるとマークが付けられたホストのサーバ オペレーティング システムを検出すると、同

種のホストのグループを識別できる場合があります。その場合、それらのホストのうちの1つに基づいたカスタム フィンガープリントを作成し、システムでそのフィンガープリントを、Nmap スキャンに基づいてそのホスト上で実行されていると判明したオペレーティング システムと関連付けるようにすることができます。可能な限り、Nmap などのサードパーティ製の静的データを入力するよりも、カスタムフィンガープリントを作成してください。カスタムフィンガープリントを使用すると、システムはホストのオペレーティング システムを継続してモニタし、必要に応じて更新できるからです。

この例では、次のことを実行します。

1. Nmap スキャン インスタンスの追加 （44 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートの使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
   - [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [ベンダーおよびバージョン情報のためのポートのプローブ オープン（Probe open ports for vendor and version information）] を有効にして、サーバ ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムで不明なオペレーティング システムがあるホストが検出されたときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**ホストの OS 情報が変更**されており、**OS 名が不明**という条件が満たされている場合にトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. ネットワーク マップ上のホストを消去し、強制的にネットワーク検出が再起動されてネットワーク マップが再構築されるようにします。
8. 1 日後か2 日後に、相関ポリシーによって生成されたイベントを検索します。Nmap 結果から、ホスト上で検出されたオペレーティング システムを分析し、システムで認識されない特定のホスト設定がネットワーク上にあるかどうか調べます。
9. 不明なオペレーティング システムがあるホストが複数検出され、Nmap 結果が同一の場合は、それらのホストの 1 つに対してカスタム フィンガープリントを作成し、将来類似のホストを識別する際に使用します。

関連トピック

Nmap 修復の作成 （49 ページ）
相関ルールの設定
Nmap スキャンの結果 （54 ページ）
クライアント用のカスタム フィンガープリントの作成 （8 ページ）
相関ポリシーの設定

例：Nmap を使用した新しいホストへの応答

この例では、新しいホストに応答するように設計された、Nmap 設定について説明します。Nmap 設定の詳細については、Nmap スキャンの管理 （43 ページ）を参照してください。

システムにより、侵入の可能性があるサブネット内で新しいホストが検出された場合、そのホストをスキャンして、そのホストの脆弱性に関する正確な情報を入手できます。

そのためには、このサブネット内に新しいホストが出現した時点で検出し、そのホスト上で Nmap スキャンを実行する修復を起動する相関ポリシーを作成してアクティブにします。

そのためには、次のことを実行します。

1. Nmap スキャン インスタンスの追加 （44 ページ）の説明に従って、スキャン インスタンスを設定します。
2. 次の設定を使用して Nmap 修復を作成します。
   - [イベントからのポートの使用（Use Port From Event）] を有効にして、新しいサーバに関連付けられたポートをスキャンします。
   - [オペレーティング システムの検出（Detect Operating System）] を有効にして、ホストのオペレーティング システムの情報を検出します。
   - [ベンダーおよびバージョン情報のためのポートのプローブ オープン（Probe open ports for vendor and version information）] を有効にして、サーバ ベンダーとバージョン情報を検出します。
   - ホストが既存であることが判明しているので、[すべてのホストをオンラインとして扱う（Treat All Hosts as Online）] を有効にします。
3. システムが特定のサブネット上で新しいホストを検出したときにトリガーされる相関ルールを作成します。このルールは、**検出イベントが発生**し、**新しいホストが検出**されたときにトリガーされる必要があります。
4. 相関ルールを組み込む相関ポリシーを作成します。
5. 相関ポリシー内で、ステップ 2 で応答として作成した Nmap 修復をステップ 3 で作成したルールに追加します。
6. 相関ポリシーをアクティブにします。
7. 新しいホストが通知されたら、ホスト プロファイルを調べて Nmap スキャンの結果を確認し、ホストに適用されている脆弱性に対処します。

このポリシーをアクティブにした後で、修復状態の表示（**[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）]**）を定期的に検査して、修復が起動された時点を調べることができます。修復の動的なスキャン ターゲットには、サーバ検出の結果としてスキャンされたホストの IP アドレスを含める必要があります。これらのホストのホスト プロファイルを調べて、Nmap によって検出されたオペレーティング システムとサーバに基づいて、対処する必要がある脆弱性がホストにあるかどうか確認します。

注意 大規模なネットワークや動的なネットワークがある場合、新しいホストの検出は頻繁に発生するので、スキャンを使用して応答するには不向きな場合があります。リソースの過負荷を避けるために、頻繁に発生するイベントへの応答として Nmap スキャンを使用しないでください。また、Nmap を使用して新しいホストのオペレーティング システムやサーバの情報を要求すると、スキャン対象のホストに対するによるそのデータのシスコ モニタリングが非アクティブになることに注意してください。

関連トピック

Nmap 修復の作成 （49 ページ）
相関ルールの設定
相関ポリシーの設定

Nmap スキャンの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap スキャンを使用するには、少なくとも 1 つの Nmap スキャン インスタンスと 1 つの Nmap 修復を設定する必要があります。Nmap スキャン ターゲットの設定はオプションです。

手順

ステップ 1 Nmap スキャンを設定します。

- Nmap スキャン インスタンスを追加します。詳細については、Nmap スキャン インスタンスの追加 （44 ページ）を参照してください。
- Nmap 修復を作成します。詳細については、Nmap 修復の作成 （49 ページ）を参照してください。
- 必要に応じて、Nmap スキャン ターゲットを追加します。詳細については、Nmap スキャン ターゲットの追加 （47 ページ）を参照してください。

ステップ 2 Nmap スキャンを実行します。

- オンデマンド Nmap スキャンを実行します。詳細については、オンデマンド Nmap スキャンの実行 （53 ページ）を参照してください。
- 自動 Nmap スキャンを設定します。詳細については、Nmap スキャンの自動化を参照してください。
- 自動 Nmap スキャンをスケジュールします。詳細については、Nmap スキャンのスケジュールを参照してください。

次のタスク

- 関連タスクを表示することで、進行中の Nmap スキャンをモニタします。タスク メッセージの表示を参照してください。
- 必要に応じて、次に示すようにスキャンを調整します。
  - Nmap スキャン インスタンスを編集します。詳細については、Nmap スキャン インスタンスの編集 （46 ページ）を参照してください。
  - Nmap スキャン ターゲットを編集します。詳細については、Nmap スキャン ターゲットの編集 （48 ページ）を参照してください。
  - Nmap 修復を編集します。詳細については、Nmap 修復の編集 （52 ページ）を参照してください。

Nmap スキャン インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

脆弱性についてネットワークをスキャンするのに使用する Nmap モジュールごとに別々のスキャン インスタンスをセットアップできます。Firepower Management Center 上のローカル Nmap モジュールか、リモートでスキャンを実行するために使用するデバイスに対してスキャン インスタンスをセットアップできます。各スキャンの結果は常に Firepower Management Center に保存されます。リモートデバイスからスキャンを実行する場合でも、この場所でスキャンを設定できます。ミッションクリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスは追加できません。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャン インスタンスを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 次のいずれかの方法を使用して Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 以下の場合、修復を追加します。

- 上記の最初の方法でリストにアクセスした場合は、[新しいインスタンスの追加（Add a New Instance）] セクションを探し、ドロップダウン リストから Nmap 修復モジュールを選択し、[追加（Add）] をクリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、[Nmap インスタンスの追加（Add Nmap Instance）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] を入力します。

ステップ 4 [説明（Description）] を入力します。

ステップ 5 オプションで、[ブラックリスト化されたスキャン ホスト（Black Listed Scan hosts）] フィールドで、このスキャンインスタンスがスキャンしないホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）
- 感嘆符（!）を使用してアドレス値の否定はできないことに注意してください。

（注） ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。

ステップ 6 オプションで、Firepower Management Center の代わりにリモート デバイスからスキャンを実行するには、そのデバイスの IP アドレスか名前を指定します。この情報は、Management Center Web インターフェイス内のそのデバイスに関する [Information] ページの [Remote Device Name] フィールドに表示されます。

ステップ 7 [作成（Create）] をクリックします。
システムがインスタンスの作成を終えると、編集モードでこのインスタンスが表示されます。

ステップ 8 必要に応じて、インスタンスに Nmap の修復を追加します。そのためには、インスタンスの [設定されている修復（Configured Remediations）] を探し、[追加（Add）] をクリックし、Nmap 修復の作成 （49 ページ）の説明に従って修復を作成します。

ステップ 9 インスタンスのリストに戻るには、[キャンセル（Cancel）] をクリックします。

（注） [スキャナ（Scanners）] オプションにより Nmap スキャンインスタンスのリストにアクセスした場合は、インスタンスの修復も併せて追加しないと追加したインスタンスは表示されません。修復が追加されていないインスタンスをすべて表示するには、[インスタンス（Instances）] メニュー オプションを使ってリストにアクセスします。

Nmap スキャン インスタンスの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

スキャン インスタンスを編集する場合、インスタンスに関連付けられている修復を表示、追加、および削除できます。インスタンス内でプロファイルが作成された Nmap モジュールを使用しなくなった場合には、Nmap スキャンインスタンスを削除します。スキャンインスタンスを削除すると、そのインスタンスを使用する修復も削除されることに注意してください。

マルチドメイン展開では、現在のドメインで作成されたスキャン インスタンスが表示されます。これは編集できます。先祖ドメインで作成されたスキャン インスタンスも表示されますが、これは編集できません。下位のドメインのスキャンインスタンスを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 次のいずれかの方法を使用して Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 編集するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 Nmap スキャン インスタンスの追加 （44 ページ）の説明に従って、スキャン インスタンスの設定を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [完了（Done）] をクリックします。

次のタスク

- 必要に応じて、スキャン インスタンスに新しい修復を追加します。次を参照してください。 Nmap 修復の作成 （49 ページ）

- 必要に応じて、インスタンスに関連付けられている修復を編集します。Nmap 修復の編集（52 ページ）を参照してください。
- 必要に応じて、インスタンスに関連付けられる修復を削除します。オンデマンド Nmap スキャンの実行 （53 ページ）を参照してください。
- 必要に応じて、その横にある削除アイコン（）をクリックして、スキャンインスタンスを削除します。

Nmap スキャン ターゲットの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmapモジュールを設定する際にスキャンターゲットを作成して保存できます。スキャンターゲットは、オンデマンドまたはスケジュール済みのスキャンの実行時にターゲットにするホストとポートを識別します。これにより、毎回新しいスキャンターゲットを作成する必要がなくなります。スキャン ターゲットには、スキャンする 1 つの IP アドレスか IP アドレスのブロック、および 1 つ以上のホスト上のポートが含まれます。Nmap ターゲットの場合、オクテット範囲による Nmap のアドレッシングや IP アドレスの範囲も使用できます。Nmap のオクテット範囲によるアドレッシングの詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

（注）

- スキャンターゲットに多数のホストが含まれている場合、スキャンに要する時間が延びる場合があります。回避策として、一度にスキャンするホストを減らしてください。
- Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。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。ホストがネットワーク マップから削除されると、Nmap スキャン結果はすべて破棄されます。
- マルチドメイン展開では、現在のドメインで作成されたスキャンターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャンターゲットも表示されますが、これは編集できません。下位のドメインのスキャンターゲットを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。
ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。
ステップ 3 [スキャン ターゲットの作成（Create Scan Target）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、このスキャン ターゲットに使用する名前を入力します。

ステップ 5 [IP 範囲（IP Range）] テキスト ボックスで、Nmap スキャンのガイドライン （38 ページ）で説明しているシンタックスを使用して、スキャンする 1 つ以上のホストを指定します。

（注） スキャン ターゲット内の IP アドレスか範囲のリストでカンマを使用した場合、ターゲットを保存する際にカンマはスペースに変換されます。

ステップ 6 [ポート（Ports）] フィールドで、スキャンするポートを指定します。

1 から 65535 までの値を使用して、次のいずれかを入力できます。

- ポート番号
- カンマで区切ったポートのリスト
- ハイフンで区切ったポート番号の範囲
- ハイフンで区切ったポート番号の複数の範囲をカンマで区切ったもの

ステップ 7 [保存（Save）] をクリックします。

関連トピック

Nmap スキャンの自動化

Nmap スキャン ターゲットの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

ヒント 修復を使用して特定の IP アドレスをスキャンするつもりがないのに、修復を起動した相関ポリシー違反にホストが関係していたためにその IP アドレスがターゲットに追加された場合は、修復の動的スキャン ターゲットを編集できます。

スキャンターゲットにリストされているホストをスキャンする必要がなくなった場合は、そのスキャン ターゲットを削除します。

マルチドメイン展開では、現在のドメインで作成されたスキャンターゲットが表示されます。これは編集できます。先祖ドメインで作成されたスキャンターゲットも表示されますが、これは編集できません。下位のドメインのスキャンターゲットを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[ターゲット（Targets）] をクリックします。

ステップ 3 編集するスキャン ターゲットの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、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 4 必要に応じて変更を加えます。詳細については、Nmap スキャン ターゲットの追加 （47 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

ステップ 6 必要に応じて、その横にある削除アイコン（）をクリックして、スキャンターゲットを削除します。

Nmap 修復の作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap 修復は、既存の Nmap スキャン インスタンスに修復を追加することによってのみ作成できます。修復では、スキャンの設定を定義します。これは相関ポリシーで応答として使用したり、オンデマンドで実行したり、スケジュール タスクとして特定の時刻に実行したりできます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。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。ホストがネットワーク マップから削除されると、Nmap スキャン結果が破棄されます。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

始める前に

- Nmap スキャン インスタンスの追加 （44 ページ）の説明に従って、Nmap スキャン インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 [設定済みの修復（Configured Remediations）] セクションで、[追加（Add）] をクリックします。

ステップ 4 [修復名（Remediation Name）] を入力します。

ステップ 5 [説明（Description）] を入力します。

ステップ 6 侵入イベント、接続イベント、ユーザイベントをトリガーする相関ルールに応じてこの修復を使用する場合は、[スキャンするイベントのアドレス（Scan Which Address(es) From Event?）] オプションを設定します。

ヒント ディスカバリイベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

（注） トラフィック プロファイルの変更に対してトリガーする相関ルールへの応答として Nmap 修復を割り当て**ないでください**。

ステップ 7 [スキャン タイプ（Scan Type）] オプションを設定します。

ステップ 8 オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン（Scan for UDP ports）] オプションで [オン（On）] を選択します。

ヒント UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

ステップ 9 相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからポートを使用（Use Port From Event）] オプションを設定します。

ステップ 10 相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン（Scan from reporting detection engine）] オプションを設定します。

ステップ 11 [高速ポート スキャン（Fast Port Scan）] オプションを設定します。

ステップ 12 [ポート範囲およびスキャン順序（Port Ranges and Scan Order）] フィールドに、デフォルトでスキャンするポートを入力します。Nmap ポート指定シンタックスを使用し、ポートをスキャンする順序で入力します。

次の形式を使用します。

- 1 から 65535 までの値を指定します。
- ポートを区切るには、カンマかスペースを使用します。
- ポート範囲を示すには、ハイフンを使用します。

- TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。

（注） 手順 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからポートを使用（Use Port From Event）] オプションによりこの設定が上書きされます。

例：

UDP トラフィックのポート 53 と 111 をスキャンしてから、TCP トラフィックのポート 21 から 25 までスキャンするには、`U:53,111,T:21-25` と入力します。

ステップ 13 開いているポートでサーバ ベンダーおよびバージョン情報をプローブするには、[ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を設定します。

ステップ 14 開いているポートをプローブすることにした場合、[サービス バージョンの強さ（Service Version Intensity）] ドロップダウン リストから数値を選択することにより、使用されるプローブの数を設定します。

ステップ 15 オペレーティング システム情報をスキャンするには、[オペレーティング システムの検出（Detect Operating System）] 設定を行います。

ステップ 16 ホスト ディスカバリが行われるかどうか、およびポートのスキャンが使用可能なホストのみに対して実行されるかどうかを決めるには、[すべてのホストをオンラインとして扱う（Treat All Hosts As Online）] を設定します。

ステップ 17 Nmap でホストの使用可能性をテストする際に使用する方法を設定するには、[ホスト ディスカバリ方式（Host Discovery Method）] ドロップダウン リストから方式を選択します。

ステップ 18 ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、選択したホスト ディスカバリ方式に適したポートのリストを、[ホスト ディスカバリ ポート リスト（Host Discovery Port List）] フィールドにカンマで区切って入力します。

ステップ 19 [デフォルト NSE スクリプト（Default NSE Scripts）] オプションを設定して、ホスト ディスカバリおよび、サーバ、オペレーティング システム、脆弱性のディスカバリに Nmap スクリプトのデフォルト セットを使用するかどうかを制御します。

ヒント デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

ステップ 20 スキャン プロセスのタイミングを設定するには、[タイミング テンプレート（Timing Template）] ドロップダウン リストからタイミング テンプレート番号を選択します。

より高速だが、包括的でないスキャンを実行する場合は大きい番号を選択し、低速で、より包括的なスキャンを実行する場合は小さい番号を選択します。

ステップ 21 [作成（Create）] をクリックします。
修復の作成が完了すると、修復が編集モードで表示されます。

ステップ 22 [完了（Done）] をクリックして、関連インスタンスに戻ります。

ステップ 23 [キャンセル（Cancel）] をクリックすると、インスタンス リストに戻ります。

関連トピック

Nmap スキャンの自動化
Nmap 修復オプション （28 ページ）

Nmap 修復の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap 修復に加えた変更は、進行中のスキャンには影響しません。新しい設定は、次回スキャンが開始されたときに有効になります。Nmap 修復が不要になったら削除します。

マルチドメイン導入では、現在のドメインで作成された Nmap 修復が表示されます。これは編集できます。先祖ドメインで作成された Nmap 修復も表示されますが、これは編集できません。下位ドメインの Nmap 修復を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 以下のいずれかの方法を使用して、Nmap スキャン インスタンスのリストにアクセスします。

- **[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**を選択します。
- **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 編集する修復にアクセスします。

- 上記の最初の方法でリストにアクセスした場合は、関連するインスタンスの横にある表示アイコン（）をクリックし、次に、[設定済み修復（Configured Remediations）] セクションで、編集する修復の横にある表示アイコンを再度クリックします。
- 上記の 2 番目の方法でリストにアクセスした場合は、編集する修復の横にある表示アイコン（）をクリックします。

ステップ 3 Nmap 修復の作成 （49 ページ）の説明に従って、必要に応じて変更を加えます。

ステップ 4 変更を保存する場合は [保存（Save）] をクリックし、保存せずに終了する場合は [完了（Done）] をクリックします。

ステップ 5 必要に応じて、その横にある削除アイコン（）をクリックして修復を削除します。

オンデマンド Nmap スキャンの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

オンデマンド Nmap スキャンは、いつでも必要なときに起動できます。スキャンする IP アドレスとポートを入力するか、既存のスキャン ターゲットを選択することで、オンデマンド スキャンのターゲットを指定できます。

Nmap によって提供されるサーバやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。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。ホストがネットワーク マップから削除されると、Nmap スキャンの結果は破棄されます。

始める前に

- 必要に応じて、Nmap スキャン ターゲットを追加します。Nmap スキャン ターゲットの追加 （47 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 スキャンの実行時に使用する Nmap 修復の横にあるスキャン アイコン（  ）をクリックします。

ステップ 3 必要に応じて、保存済みのスキャン ターゲットを使用してスキャンする場合は、[保存済ターゲット（Saved Targets）] ドロップダウンリストからターゲットを選択して、[ロード（Load）] をクリックします。

（注） スキャン ターゲットを追加するには、ダイアログの上部にある編集アイコン（  ）をクリックします。

ステップ 4 [IP 範囲（IP Range(s)）] フィールドで、スキャンするホストの IP アドレスを指定するかロードされたリストを変更します。

（注）

- IPv4 アドレスのホストの場合は、複数の IP アドレスをカンマで区切って指定するか、CIDR 表記を使用できます。感嘆符（!）を前に挿入して IP アドレスを否定することもできます。
- IPv6 アドレスのホストの場合は、厳密な IP アドレスを使用します。範囲はサポートされていません。

ステップ 5 [ポート（Ports）] フィールドで、スキャンするポートを指定するか、ロードされたリストを変更します。

ポート番号、カンマで区切ったポートのリスト、ハイフンで区切ったポート番号の範囲を入力できます。

ステップ 6 マルチドメイン展開では、[ドメイン（Domain）] フィールドを使用して、スキャンを実行するリーフ ドメインを指定します。

ステップ 7 [今すぐスキャン（Scan Now）] をクリックします。

次のタスク

- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示を参照）。

関連トピック

Nmap スキャンの自動化
Firepower システムの IP アドレス表記法
検索でのポート

Nmap スキャンの結果

進行中の Nmap スキャンをモニタし、Firepower システムによって実行されたスキャンの結果あるいは Firepower システム外部で行われたスキャンの結果をインポートして、スキャン結果を表示および分析することができます。

ローカル Nmap モジュールを使用して作成したスキャン結果を、レンダリングされたページとしてポップアップ ウィンドウで表示できます。Nmap 結果ファイルを raw XML 形式でダウンロードすることもできます。

Nmap によって検出されたオペレーティング システムやサーバの情報を、ホスト プロファイルやネットワーク マップ内で参照することもできます。ホストのスキャンが生成するサーバ情報がフィルタ除去されているかクローズ状態のポートのサーバに関する情報の場合、または、スキャンが収集した情報がオペレーティング システム情報やサーバのセクションに含めることができない情報の場合、それらの結果は、ホスト プロファイルの [Nmap スキャン結果（Nmap Scan Results）] セクションに含めることができます。

Nmap スキャン結果の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Nmap スキャンが完了したら、スキャン結果のテーブルを表示できます。

ユーザは検索する情報に応じて結果のビューを操作することができます。スキャン結果にアクセスすると表示されるページは、使用するワークフローに応じて異なります。定義済みのワークフローを使用できます。このワークフローにはスキャン結果のテーブル ビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

http://insecure.org で使用可能な Nmap バージョン 1.01 DTD を使用して Nmap の結果をダウンロードして表示することができます。

スキャン結果をクリアすることもできます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[スキャン結果（Scan Results）] をクリックします。

ステップ 3 次の選択肢があります。

- イベント時間の制約の説明に従って、時間範囲を調整します。
- カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。
- スキャン結果をレンダリングされたページとしてポップアップ ウィンドウで表示するには、スキャン ジョブの横にある [表示（View）] をクリックします。
- テキスト エディタで raw XML コードを表示できるようにスキャン結果ファイルのコピーを保存するには、スキャン ジョブの横の [ダウンロード（Download）] をクリックします。
- スキャン結果をソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- 表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にしたカラムをビューに戻すには、展開の矢印をクリックして検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用を参照してください。
- スキャン インスタンスや修復を設定するには、ツールバーの [スキャナ（Scanners）] をクリックしてください（Nmap スキャンの管理 （43 ページ）を参照）。
- ワークフロー ページ内およびワークフロー ページ間で移動するには、ワークフロー ページのナビゲーション ツールを参照してください。

- その他のイベント ビューに移動して関連するイベントを表示するには、[ジャンプ（Jump to）] ドロップダウン リストから、表示するイベント ビューの名前を選択します。
- スキャン結果を検索するには、該当するフィールドに検索条件を入力します。

関連トピック

Nmap スキャン結果のフィールド （56 ページ）

Nmap スキャン結果のフィールド

Nmap スキャンを実行すると、Firepower Management Center でデータベース内のスキャン結果が収集されます。次の表に、表示および検索できるスキャン結果テーブルのフィールドを示します。

表 *3*: スキャン結果のフィールド

フィールド	説明
開始時間（Start Time）	この結果を作成したスキャンの開始日時。
終了時間（End Time）	この結果を作成したスキャンの終了日時。
ターゲット（Target）	この結果を作成したスキャンのスキャン ターゲットの IP アドレス（DNS 解決が有効になっている場合はホスト名）。
Scan Type	この結果を作成したスキャンのタイプを示す、`Nmap` またはサードパーティのスキャナ名。
スキャン モード（Scan Mode）	この結果を作成したスキャンのモード： • [オンデマンド（On Demand）]：オン デマンドで実行されたスキャンからの結果。 • [インポート済み（Imported）]：別のシステムでスキャンされて Firepower Management Center にインポートされた結果。 • [スケジュール済み（Scheduled）]：スケジュール済みタスクとして実行されたスキャンからの結果。
結果	スキャンの結果。
ドメイン	スキャン ターゲットのドメイン。このフィールドは、マルチドメイン展開の場合にのみ存在します。

関連トピック

イベントの検索

Nmap スキャン結果のインポート

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Discovery Admin

Firepower システムの外部で実行した Nmap スキャンによって作成された XML 結果ファイルをインポートできます。以前に Firepower システムからダウンロードした XML 結果ファイルもインポートできます。Nmap スキャン結果をインポートする場合、結果ファイルは XML 形式で、Nmap バージョン 1.01 DTD に準拠している必要があります。Nmap 結果の作成と Nmap DTD の詳細については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap がホスト プロファイルに結果を追加できるようにするには、その前にホストがネットワーク マップ内に存在している必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）]**を選択します。

ステップ 2 ツールバーで、[結果のインポート（Import Results）] をクリックします。

ステップ 3 マルチドメイン展開では、インポートされた結果の保存場所を指定するために、[ドメイン（Domain）] ドロップダウンリストからリーフ ドメインを選択します。

ステップ 4 [参照（Browse）] をクリックして、結果ファイルに移動します。

ステップ 5 [インポートの結果（Import Results）] ページに戻ったら、[インポート（Import）] をクリックして結果をインポートします。