アプリケーションの検出

次のトピックでは、Firepower システム アプリケーション検出について説明します。

概要：アプリケーション検出

システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーションを制御するために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web* アプリケーション

システムは、ディテクタに指定されている特性に従って、ネットワーク トラフィック内のアプリケーションを識別します。たとえば、システムはパケット ヘッダーに含まれる ASCII パターンによってアプリケーションを確認できます。加えて、Secure Socket Layer（SSL）プロトコル

ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。

アプリケーションディテクタの供給元には次の 2 つがあります。

- システム提供ディテクタ。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します。

  アプリケーション（およびオペレーティングシステム）に対して使用できるシステム提供ディテクタは、インストールされているシステムソフトウェアのバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。

- カスタム アプリケーション プロトコル ディテクタ。Web アプリケーション、クライアント、アプリケーションプロトコルを検出するためにユーザーが作成するディテクタです。

また、暗黙的アプリケーション プロトコル検出を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーションプロトコルの存在を推測するものです。

ネットワーク検出ポリシーで定義されているように、システムはモニタ対象ネットワーク内のホスト上で動作しているアプリケーションプロトコルだけを識別します。たとえば、モニタされていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、モニタされているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーションプロトコルを肯定的に識別できます。

モニタ対象ホストが非モニタ対象サーバに接続するために使用するクライアントをシステムで識別できる場合、システムはクライアントの対応するアプリケーションプロトコルを識別することができますが、そのプロトコルをネットワークマップに追加することはしません。アプリケーション検出が発生するためには、クライアントセッションにサーバからの応答が含まれている必要があることに注意してください。

システムは、検出した各アプリケーションの特徴を把握します（アプリケーションルールの条件を参照）。システムはこれらの特徴を使用して、アプリケーション フィルタと呼ばれるアプリケーションのグループを作成します。アプリケーション フィルタは、アクセス制御するため、およびレポートとダッシュボードウィジェットで使用する検索結果とデータを制限するために使用されます。

また、エクスポートした NetFlow レコード、Nmap のアクティブ スキャン、ホスト入力機能を使用してアプリケーション ディテクタ データを補完することもできます。

関連トピック

アプリケーション ディテクタの基本 （3 ページ）

アプリケーション ディテクタの基本

システムは、アプリケーションディテクタを使用して、ネットワーク上で一般的に使用されるアプリケーションを識別します。[ディテクタ（Detectors）] ページ（**Policies** > **Application Detectors**）を使用してディテクタ リストを表示し、検出機能をカスタマイズします。

ディテクタまたはその状態（アクティブ/非アクティブ）を変更できるかどうかは、そのタイプによって異なります。システムは、アクティブなディテクタのみを使用して、アプリケーション トラフィックを分析します。

（注） シスコが提供するディテクタは、システムおよび VDB のアップデートによって変更される可能性があります。更新されたディテクタに関する情報については、リリース ノートおよびアドバイザリを参照してください。

（注） Firepower アプリケーションの識別のために、ポートは意図的にリストされていません。シスコのアプリケーションのいずれについても、アプリケーションの関連ポートは報告されません。これは、ほとんどのアプリケーションはポートに依存しないためです。シスコのプラットフォームの検出機能では、ネットワークのどのポートで実行されているサービスでも識別できます。

シスコが提供する内部ディテクタ

内部ディテクタは、クライアント、Web アプリケーション、およびアプリケーション プロトコルのトラフィック用の特別なディテクタ カテゴリです。内部ディテクタはシステム アップデートによって配信され、常にオンになっています。

アプリケーションがクライアント関連のアクティビティを検出するように設計された内部ディテクタと照合する場合で、特定のクライアントディテクタがない場合は、汎用クライアントが報告される場合があります。

シスコが提供するクライアント ディテクタ

クライアントディテクタは、クライアント トラフィックを検出し、VDB またはシステム アップデートを介して配信されるか、または Cisco Professional サービスによってインポート用に提供されます。クライアントディテクタを有効または無効にすることができます。インポートしたクライアント ディテクタのみエクスポートできます。

シスコが提供する Web アプリケーション ディテクタ

Web アプリケーションディテクタは、HTTP トラフィック ペイロード内の Web アプリケーションを検出し、VDB またはシステム アップデートを介して配信されます。Web アプリケーション ディテクタは常にオンになっています。

シスコが提供するアプリケーション プロトコル（ポート）ディテクタ

ポートベースのアプリケーション プロトコル ディテクタは、ウェルノウン ポートを使用してネットワーク トラフィックを識別します。これらはVDBまたはシステム アップデートを介して配信されるか、またはCisco Professionalサービスによってインポート用に提供されます。アプリケーション プロトコル ディテクタを有効または無効にしたり、カスタム ディテクタの基礎として使用するためにディテクタ定義を表示することができます。

シスコが提供するアプリケーション プロトコル（**Firepower**）ディテクタ

Firepower ベースのアプリケーション プロトコル ディテクタは、Firepowerアプリケーション フィンガープリントを使用してネットワーク トラフィックを分析し、VDB またはシステム アップデートを介して配信されます。アプリケーション プロトコル ディテクタを有効または無効にすることができます。

カスタム アプリケーション ディテクタ

カスタムアプリケーションディテクタはパターンベースです。クライアント、Webアプリケーション、またはアプリケーションプロトコルのトラフィックからのパケット内のパターンを検出します。インポートされたカスタム ディテクタを完全に制御できます。

Web インターフェイスでのアプリケーション プロトコルの識別

次の表に、検出されたアプリケーションプロトコルの識別方法の概略を示します。

表 *1*: システムのアプリケーションプロトコルの識別

ID	説明
アプリケーション プロトコル名	Firewall Management Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlowデータを使用して識別され、`/etc/sf/services`にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された

ID	説明
pending	Firewall Management Centerは、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを pending として識別します。 多くの場合、システムが保留中のアプリケーションを識別するには、より多くの接続データを収集して分析する必要があります。 [アプリケーションの詳細（Application Details）] および [サーバ（Servers）] テーブルやホスト プロファイルで pending ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック（検出されたクライアントまたは Web アプリケーション トラフィックから推論されたトラフィック以外）が検出されたアプリケーション プロトコルだけです。
unknown	Firewall Management Centerは、以下の場合にアプリケーションプロトコルを unknown として識別します。 • アプリケーションがシステムのいずれのディテクタとも一致しない。 • アプリケーションプロトコルが NetFlow データを使用して識別されたが、/etc/sf/services にポートとアプリケーションプロトコルの関連付けが存在しない。 • Snortがセッションを閉じたが、デバイスにまだセッションが残っている。この場合、トラフィックはファイアウォールを通過できますが、アプリケーションは検出されません。
空白	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細（Application Details）] および [サーバー（Servers）] テーブルとホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

非監視対象サーバにアクセスするために監視対象ホストが使用しているクライアントをシステムが識別できる場合、Firewall Management Centerはその接続でクライアントに対応するアプリケーションプロトコルが使用されていると推測します（システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーションプロトコル情報が含まれていません）。

暗黙的アプリケーション プロトコル検出と呼ばれるこのプロセスの結果は次のようになります。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ（Servers）] テーブルに表示されません。加えて、これらの

アプリケーションプロトコルの検出を基準にして、検出イベントアラートまたは相関ルールをトリガーすることはできません。

- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホストプロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、アプリケーションプロトコル情報が接続内に存在するかどうかに対する相関イベントをトリガーできます。また、接続ログ内のアプリケーションプロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバー上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション検出に関する特別な考慮事項

SFTP

SFTP トラフィックを検出するためには、同じルールが SSH も検出する必要があります。

Squid

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- モニタ対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- モニタ対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- 監視対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: ヘッダー フィールドを除去するように設定されている場合

SSL アプリケーション検出

システムは、Secure Socket Layer（SSL）セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するアプリケーション ディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合には SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の **Client** フィールドに `SSL client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSL アプリケーション トラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホスト パターンからのクライアントまたは Web アプリケーションと照合できます。システムが特定のクライアントを識別すると、`SSL client` をそのクライアントの名前に置き換えます。

SSL アプリケーション トラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーション データではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホスト パターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックを監視するアクセス コントロール ルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーでモニタできます。アクセス コントロール ポリシーの設定によって、トラフィックが識別されるかどうかが決まります。SSL アプリケーションの検出を識別するには、アプリケーション ディテクタ リストで、または、アプリケーション条件をアクセス コントロール ルールに追加するときに、`SSL protocol` タグでフィルタ処理します。

参照先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト（通常は、アドバタイズメント サーバ）に参照する場合があります。ネットワーク上で発生するトラフィック参照のコンテキストをわかりやすくするために、システムは、参照セッションに対するイベント内の [Web アプリケーション（Web Application）] フィールドにトラフィックを参照した Web アプリケーションを列挙します。VDB に既知の照会先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、照会元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP 参照元（HTTP Referrer）] イベント フィールドに表示されます。

イベントでは、参照元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は参照先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。参照元 Web アプリケーションが検出されない場合、ホストが自身を参照している場合、または参照がチェインしている場合は、参照先アプリケーションが Web アプリケーションとして表示される場合もあります。ダッシュボードでは、Web アプリケーションの接続カウントとバイト カウントに、Web アプリケーションが参照先のトラフィックに関連付けられたセッションが含まれます。

照会先トラフィックに対して明示的に機能するルールを作成する場合は、照会元アプリケーションではなく、照会先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から参照される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

Snort 3 でのアプリケーション検出

（注） Snort 3 は、すべてのトラフィックを監視するために AppID を必要とする他の構成が AC ポリシーに存在しない場合、ネットワーク検出ポリシーフィルタで定義されている特定のネットワークサブネットでのみ AppID インスペクションを有効にするという点で、Snort 2 と同等になりました。

Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。アプリケーション検出を無効にするには、次の手順を実行します。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control** を選択し、ポリシーの編集をクリックし、アプリケーション ルールを削除します。

ステップ 2 **Policies** > **Access Control heading** > **Decryption** を選択し、[削除（delete）] をクリックして SSL ポリシーを削除します。

ステップ 3 **Policies** > **Network Discovery** を選択し、[削除（Delete）] をクリックしてネットワーク検出ポリシーを削除します。

ステップ 4 **Policies** > **Access Control heading** > **Access Control** を選択し、編集するポリシーの **Edit** (✎) をクリックします。次に**[セキュリティインテリジェンス（Security Intelligence）]** > **[URL（URLs）]** タブを選択して、URL の許可リストまたはブロックリストを削除します。

ステップ 5 デフォルトの DNS ルールは削除できないため、**Policies** > **Access Control heading** > **DNS** を選択し、編集をクリックして、有効になっているボックスをオフにし、DNS ポリシーを無効にします。

ステップ 6 アクセス コントロール ポリシーの [詳細（Advanced）] 設定で、[Threat Intelligence Directorを有効にする（Enable Threat Intelligence Director）] および [DNSトラフィックへのレピュテーショ

ン適用を有効にする（Enable reputation enforcement on DNS traffic）] オプションを無効にします。

ステップ 7 アクセス コントロール ポリシーを保存して展開します。

アプリケーション検出の要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Discovery Admin

カスタム アプリケーション ディテクタ

ネットワーク上でカスタムアプリケーションを使用する場合、アプリケーションの識別に必要な情報をシステムに提供するカスタム Web アプリケーション、クライアント、またはアプリケーションプロトコルディテクタを作成します。アプリケーションディテクタの種類は、[プロトコル（Protocol）]、[タイプ（Type）]、および [検出方向（Direction）] フィールドで選択した内容によって決まります。

システムがサーバ トラフィックでアプリケーション プロトコルの検出および識別を開始するように、クライアントセッションにサーバからの応答パケットを含める必要があります。UDP トラフィックの場合、応答パケットの送信元がサーバとして指定されることに注意してください。

すでに別の Firewall Management Center にディテクタを作成している場合、そのディテクタをエクスポートして、この Firewall 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ディテクタを編集できます。カスタム ディテクタおよび Cisco Professional サービスが提供するディテクタをエクスポートおよびインポートすることができます。ただし、シスコが提供するその他の種類のディテクタをエクスポートおよびインポートすることは**できません**。

カスタムアプリケーションディテクタおよびユーザー定義アプリケーション フィールド

次のフィールドを使用して、カスタム アプリケーション ディテクタおよびユーザー定義アプリケーションを設定できます。

カスタム アプリケーション ディテクタ フィールド：概要

基本および高度なカスタム アプリケーション ディテクタを設定するには、次のフィールドを使用します。

アプリケーション プロトコル（Application Protocol）

検出するアプリケーションプロトコル。これには、システムが提供するアプリケーションまたはユーザー定義のアプリケーションを指定できます。

アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグを使用してアプリケーション プロトコルを選択するか、作成する必要があります。

説明

アプリケーション ディテクタの説明。

[名前（Name）]

アプリケーション ディテクタの名前。

ディテクタ タイプ（Detector Type）

ディテクタのタイプ（[基本（Basic）] または [高度（Advanced）]）。基本的なアプリケーションディテクタは、一連のフィールドとして Web インターフェイスで作成されます。高度なアプリケーション ディテクタは、外部で作成され、カスタム .lua ファイルとしてアップロードされます。

カスタムアプリケーションディテクタ（Custom Application Detector）フィールド：検出パターン

基本的なカスタム アプリケーション ディテクタの検出パターンを設定するには、次のフィールドを使用します。

方向（Direction）

ディテクタが検出するトラフィックの送信元。[クライアント（Client）] または [サーバー（Server）]。

オフセット（Offset）

システムがパターンの検索を開始する必要がある、パケット ペイロードの先頭からのパケットの場所（バイト単位）。

パケット ペイロードは 0 バイトから始まるため、パケット ペイロードの先頭から数えたバイト数から 1 を減算することでオフセットを計算します。たとえば、パケットの 5 桁目

のビットパターンを検索するには、[オフセット（Offset）]フィールドに「4」と入力します。

パターン

パターン文字列は、選択した [タイプ（Type）] に関連付けられます。

ポート

ディテクタが検出するトラフィックのポート。

プロトコル

検出するプロトコル。選択するプロトコルによって、[タイプ（Type）]フィールドが表示されるか [URL（URL）] フィールドが表示されるかが決まります。

プロトコル（および、場合によっては、[タイプ（Type）]フィールドと [方向（Direction）] フィールドの後続の選択）によって、作成するアプリケーションディテクタのタイプ（Web アプリケーション、クライアント、またはアプリケーションプロトコル）が決まります。

ディテクタ タイプ（**Detector Type**）	プロトコル	タイプ（**Type**）または 方向（**Direction**）
Web アプリケーション（Web Application）	HTTP	[タイプ（Type）] は [コンテンツ タイプ（Content Type）] または [URL（URL）] です。
	RTMP	任意（Any）
	SSL	任意（Any）
クライアント	HTTP	[タイプ（Type）] は [ユーザー エージェント（User Agent）] です。
	SIP	任意（Any）
	TCP または UDP	[方向（Direction）] は [クライアント（Client）] です。
アプリケーション プロトコル（Application Protocol）	TCP または UDP	[方向（Direction）] は [サーバー（Server）] です。

タイプ（Type）

入力したパターン文字列のタイプ。表示されるオプションは、選択した [プロトコル（Protocol）] によって決まります。プロトコルとして [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりに [URL（URL）] フィールドが表示されます。

（注） [タイプ（Type）] として [ユーザー エージェント（User Agent）] を選択すると、システムはアプリケーションの [タグ（Tag）] を **User-Agent Exclusion** に自動的に設定します。

タイプの選択	文字列特性
Ascii	文字列は ASCII でエンコードされます。
Common Name	文字列は、サーバー応答メッセージ内の commonName フィールドの値です。
コンテンツ タイプ（Content Type）	文字列は、サーバー応答ヘッダー内のコンテンツ タイプ フィールドの値です。
16 進数	文字列は、16 進表記です。
組織	文字列は、サーバー応答メッセージ内の organizationName フィールドの値です。
SIP サーバー	文字列は、メッセージ ヘッダー内の From フィールドの値です。
SSL ホスト（SSL Host）	文字列は、ClientHello メッセージ内の server_name フィールドの値です。
URL	文字列は URL です。 （注） ディテクタは、ユーザーが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。
ユーザー エージェント（User Agent）	文字列は、GET リクエスト ヘッダー内の user-agent フィールドの値です。これは SIP プロトコルにも使用可能であり、文字列が SIP メッセージ ヘッダー内の User-Agent フィールドの値であることを示します。

URL

RTMP パケットの C2 メッセージ内の swfURL フィールドの完全な URL または URL のセクション。[プロトコル（Protocol）] として [RTMP（RTMP）] を選択すると、[タイプ（Type）] フィールドの代わりにこのフィールドが表示されます。

（注） ディテクタは、ユーザーが入力する文字列が URL の完全なセクションであると想定します。たとえば、**cisco.com** と入力した場合、**www.cisco.com/support** や **www.cisco.com** と一致しますが、**www.wearecisco.com** とは一致しません。

ユーザー定義のアプリケーション フィールド

基本および高度なカスタム アプリケーション ディテクタでユーザー定義のアプリケーションを設定するには、次のフィールドを使用します。

ビジネスとの関連性（Business Relevance）

アプリケーションが娯楽ではなく組織のビジネス活動のコンテキストで使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

カテゴリ

アプリケーションの最も基本的な機能を表す一般的な分類。

説明

アプリケーションの説明。

[名前（Name）]

アプリケーションの名前。

リスク（Risk）

アプリケーションが組織のセキュリティ ポリシーに対抗する目的で使用される可能性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）] または [非常に低い（Very Low）]。アプリケーションを最も的確に説明するオプションを選択します。

タグ（Tags）

アプリケーションに関する追加情報を提供する 1 つ以上の事前定義されたタグ。アプリケーションを（アイデンティティ ルールで設定された）アクティブな認証から除外できるようにする場合は、**User-Agent Exclusion** タグをアプリケーションに追加する必要があります。

カスタム アプリケーション ディテクタの設定

基本または高度なカスタム アプリケーション ディテクタを設定できます。

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 [カスタム ディテクタの作成（Create Custom Detector）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] を入力します。

ステップ 4 アプリケーション ドロップダウン リストから [アプリケーションプロトコル（Application Protocol）] を選択します。次の選択肢があります。

- 既存のアプリケーションプロトコルのディテクタを作成する場合（たとえば、非標準ポートで特定のアプリケーション プロトコルを検出する場合）、ドロップダウン リストからアプリケーション プロトコルを選択します。
- ユーザー定義アプリケーションのディテクタを作成する場合は、ユーザー定義アプリケーションを作成する （15 ページ）に示されている手順に従います。

ステップ 5 [ディテクタタイプ（Detector Type）] として [基本（Basic）] または [高度（Advanced）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [検出パターン（Detection Patterns）]、[検出基準（Detection Criteria）]、または [Encrypted Visibility Engineのプロセス割り当て（Encrypted Visibility Engine Process Assignments）] を設定します。

- 基本ディテクタを設定する場合は、基本ディテクタでの検出パターンの指定 （16ページ）の説明に従って、プリセットした [検出パターン（Detection Patterns）] を指定します。
- 高度なディテクタを設定する場合は、高度なディテクタでの検出条件の指定 （17ページ）の説明に従って、カスタム [検出基準（Detection Criteria）] を指定します。
- Encrypted Visibility Engine（EVE）検出器を設定している場合は、この章の「*EVE* のプロセス割り当ての指定」で説明されているように、カスタム EVE プロセス割り当てを指定します。

注意
高度なカスタムディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

ステップ 8 必要に応じて、カスタム アプリケーション プロトコル ディテクタのテスト （19 ページ）の説明に従って、[パケット キャプチャ（Packet Captures）] を使用して新しいディテクタをテストします。

ステップ 9 [保存（Save）] をクリックします。

（注）
アクセス コントロール ルールにアプリケーションを含めると、ディテクタは自動的にアクティブにされ、使用中は非アクティブにできません。

次のタスク

- ディテクタのアクティブおよび非アクティブの設定 （23 ページ）の説明に従ってディテクタをアクティブにします。

関連トピック

カスタム アプリケーション ディテクタおよびユーザー定義アプリケーション フィールド（10 ページ）

ユーザー定義アプリケーションを作成する

ここで作成するアプリケーション、カテゴリ、およびタグは、アクセス コントロール ルールやアプリケーション フィルタ オブジェクト マネージャで使用できます。

注意 ユーザー定義アプリケーションを作成すると、展開プロセスを経由することなく、ただちにSnort プロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

始める前に

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [カスタムのアプリケーションディテクタを作成する（Create A Custom Application Detector）] ダイアログボックスで、[アプリケーション（Application）] フィールドの横にある **Add** (＋) をクリックします。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 [説明（Description）] を入力します。

ステップ 4 [ビジネスとの関連性（Business Relevance）] を選択します。

ステップ 5 [リスク（Risk）] を選択します。

ステップ 6 [カテゴリ（Categories）] の横にある [追加（Add）] をクリックしてカテゴリを追加し、新しいカテゴリの名前を入力するか、または [カテゴリ（Categories）] ドロップダウン リストから既存のカテゴリを選択します。

ステップ 7 タグの横にある **[追加（Add）]** をクリックして、新しいタグを入力するか、**[タグ（Tags）]** ドロップダウンリストで既存のタグを選択します。

（注）
カスタマイズされたアプリケーション検出器ドメインをポリシーベースルーティングに関連付けるには、**[タグ（Tags）]** リストから [NSG] を選択する必要があります。

ステップ 8 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

カスタム アプリケーション ディテクタおよびユーザー定義アプリケーション フィールド（10 ページ）

基本ディテクタでの検出パターンの指定

アプリケーション プロトコルのパケット ヘッダーで特定のパターン文字列を検索するよう、カスタム アプリケーション プロトコル ディテクタを設定できます。また、複数のパターンを検索するようにディテクタを設定することもできます。この場合は、アプリケーションプロトコルのトラフィックは、アプリケーションプロトコルを確実に識別するため、ディテクタのすべてのパターンとマッチングさせる必要があります。

アプリケーション プロトコル ディテクタは、オフセットを使用して ASCII または 16 進数のパターンを検索できます。

始める前に

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [検出パターン（Detection Patterns）] セクションで、[追加（Add）] をクリックします。
ステップ 2 [アプリケーション（Application）] ドロップダウンリストからプロトコルタイプを選択します。
ステップ 3 [タイプ（Type）] ドロップダウンリストからパターンタイプを選択します。
ステップ 4 指定した [タイプ（Type）] に一致する [パターン（Pattern）] 文字列を入力します。
ステップ 5 オプションで、[オフセット（Offset）] を入力します（バイト単位）。

ステップ 6 オプションで、使用するポートに基づいてアプリケーションプロトコルのトラフィックを指定するには、1 から 65535 までのポートを [ポート（Port(s)）] フィールドに入力します。複数のポートを使用する場合は、カンマで区切ります。

ステップ 7 [方向（Direction）] : [クライアント（Client）] または [サーバー（Server）] をクリックします。

ステップ 8 [OK] をクリックします。

ヒント
パターンを削除する場合は、削除するパターンの横にある **Delete** ( ) をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

高度なディテクタでの検出条件の指定 （17 ページ）

高度なディテクタでの検出条件の指定

注意 高度なカスタムディテクタは複雑で、有効な .lua ファイルを作成すること以外の知識も必要になります。ディテクタを誤って設定すると、パフォーマンスや検出機能にマイナスの影響を与える可能性があります。

注意 信頼できないソースから .lua ファイルをアップロードしないでください。

カスタム .lua ファイルには、カスタムアプリケーションのディテクタ設定を含めます。カスタム .lua ファイルを作成するには、lua プログラミング言語に関する高度な知識とシスコの C-lua API に関する経験が求められます。以下を使用して、.lua ファイルを準備することを強くお勧めします。

- lua プログラミング言語に関するサードパーティの説明書と参考資料
- オープン ソース ディテクタ開発者ガイド： https://www.snort.org/downloads
- OpenAppID Snort コミュニティ リソース： http://blog.snort.org/search/label/openappid

（注） システムは、システム コールまたはファイル I/O を参照する .lua ファイルをサポートしていません。

始める前に

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。
- 該当する .lua ファイルをダウンロードし、内容を調べることによって、有効な .lua ファイルを作成する準備を進めます。ディテクタ ファイルのダウンロードの詳細については、ディテクタ詳細情報の表示またはダウンロード （20 ページ）を参照してください。
- カスタム アプリケーションのディテクタ設定を含む有効な .lua ファイルを作成します。

手順

ステップ 1 高度なカスタム アプリケーション ディテクタの [ディテクタの作成（Create Detector）] ページにある [検出条件（Detection Criteria）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [参照...（Browse...）] をクリックして、**.lua** ファイルに移動し、アップロードします。

ステップ 3 [OK] をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

関連トピック

基本ディテクタでの検出パターンの指定 （16 ページ）

EVE のプロセス割り当ての指定

暗号化された可視性エンジン（EVE）で検出されたプロセスを新しいアプリケーションか既存のアプリケーションにマッピングするように、独自のカスタム アプリケーション ディテクタを設定できます。

始める前に

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を開始します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [暗号化された可視性エンジンのプロセス割り当て（Encrypted Visibility Engine Process Assignments）] セクションで、[追加（Add）] をクリックします。

ステップ 2 [プロセス名（Process Name）] と [最小プロセス確実性（Minimum Process Confidence）] の値を入力します。

（注）
[プロセス名（Process Name）] フィールドにテキストを入力できますが、このフィールドでは大文字と小文字が区別されます。この値は、EVE で検出された正確なプロセス名と一致している必要があります。[最小プロセス確実性（Minimum Process Confidence）] には、0 ～ 100 までの任意の数値を指定できます。ここで指定するのは、接続イベントの [暗号化された可視性プロセスの確実性スコア（ncrypted Visibility Process Confidence Score）] フィールドに表示される数値です。

[暗号化された可視性プロセスの確実性スコア（Encrypted Visibility Process Confidence Score）] フィールドの詳細については、『Cisco Firepower Management Center Administration Guide』の「*Connection and Security Intelligence Event Fields*」セクションを参照してください。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [アプリケーションディテクタリスト（Application Detector listing）] ページで、作成したディテクタをアクティブ化します。詳細については、ディテクタ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。ディテクタをアクティブにすると、Firewall Management Center に登録されているすべての FTD にディテクタファイルがプッシュされます。

次のタスク

- カスタム アプリケーション ディテクタの設定（13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

カスタム アプリケーション プロトコル ディテクタのテスト

検出するアプリケーションプロトコルからのトラフィックを持つパケットが格納されたパケット キャプチャ（pcap）ファイルが存在する場合、その pcap ファイルに対してカスタム アプリケーション プロトコル ディテクタをテストできます。シスコでは、不要なトラフィックのない単純でクリーンな pcap ファイルを使用することをお勧めします。

pcap ファイルは 256 KB 以下でなければなりません。それより大きい pcap ファイルに対してディテクタのテストを試行すると、Firewall Management Center は自動的にファイルを切り捨

て、不完全なファイルをテストします。ディテクタをテストするためにファイルを使用する前に、pcap の未解決のチェックサムを修正する必要があります。

始める前に

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタを設定します。

手順

ステップ 1 [ディテクタの作成（Create Detector）] ページの [パケット キャプチャ（Packet Captures）] セクションで、[追加（Add）] をクリックします。

ステップ 2 ポップアップ ウィンドウで pcap ファイルを参照し、[OK] をクリックします。

ステップ 3 pcap ファイルの内容に対してディテクタをテストするには、pcap ファイルの横にある評価アイコンをクリックします。メッセージに、テストが成功したかどうかが示されます。

ステップ 4 必要に応じて手順 1 ～ 3 を繰り返し、その他の pcap ファイルに対してディテクタをテストします。

ヒント

pcap ファイルを削除するには、削除するファイルの横にある **Delete** ( ) をクリックします。

次のタスク

- カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、カスタム アプリケーション プロトコル ディテクタの設定を続けます。トラフィックを分析するためにシステムがディテクタを使用できるようにするには、その前に、ディテクタを保存してアクティブにする必要があります。

ディテクタ詳細情報の表示またはダウンロード

ディテクタ リストを使用して、アプリケーション ディテクタの詳細を表示（すべてのディテクタ）したり、ディテクタの詳細をダウンロード（カスタム アプリケーション ディテクタのみ）したりできます。

手順

ステップ 1 アプリケーション ディテクタの詳細を表示するには、次のいずれかを実行します。

- 関連する VDB バージョンについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html の『*Cisco Firepower Application Detector Reference*』[英語] を参照してください。
- a. **Policies** > **Application Detectors** を選択します。

  b. リストをフィルタ処理して、特定のディテクタを検索します。

  c. **Information**( ) をクリックします。

ステップ 2 カスタム アプリケーション ディテクタのディテクタ詳細をダウンロードするには、**Download** ( ) 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、設定が先祖ドメインに属しているか、またはユーザが必要な権限を持っていません。

ディテクタ リストのソート

[ディテクタ（Detectors）] ページには、デフォルトで名前のアルファベット順にディテクタがリストされます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 該当する列見出しをクリックします。

ディテクタ リストのフィルタリング

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 ディテクタ リストのフィルタ グループ （22 ページ）に記載されているフィルタ グループの1つを展開し、フィルタの横にあるチェックボックスを選択します。グループ内のすべてのフィルタを選択するには、グループ名を右クリックし、[すべて選択（Check All）] を選択します。

ステップ 3 あるフィルタを削除するには、[フィルタ（Filters）] フィールドにあるフィルタの名前の**Remove** ( )をクリックするか、フィルタリストでフィルタを無効にします。グループ内のすべてのフィ

ルタを削除するには、グループ名を右クリックし、[すべて選択解除（Uncheck All）] を選択します。

ステップ 4 すべてのフィルタを削除するには、検出機能に適用されるフィルタ リストの横の [すべてクリア（Clear all）] をクリックします。

ディテクタ リストのフィルタ グループ

複数のフィルタ グループを別個にまたは組み合わせて使用し、ディテクタのリストをフィルタリングすることができます。

名前（Name）

ユーザが入力した文字列を含む名前または説明でディテクタを検索します。文字列には任意の英数字または特殊文字を含めることができます。

カスタム フィルタ（Custom Filter）

オブジェクト管理ページで作成したカスタム アプリケーション フィルタに一致するディテクタを検索します。

作成者（Author）

ディテクタを作成したユーザに照らしてディテクタを検索します。次によってディテクタをフィルタリングできます。

- カスタム ディテクタを作成またはインポートした個々のユーザ
- Cisco。これは、個別にインポートされたアドオン ディテクタを除く、シスコが提供するすべてのディテクタを表します（ディテクタをインポートした場合、そのユーザはそのディテクタの作成者になります）。
- 任意のユーザ（Any User）。これは、によって提供されたのではないすべてのディテクタを表します。

状態（State）

状態（つまり、アクティブまたは非アクティブ）に照らしてディテクタを検索します。

タイプ

アプリケーション ディテクタの基本 （3 ページ）に示すように、ディテクタ タイプに従ってディテクタを検索します。

プロトコル

ディテクタが検査するトラフィック プロトコルに照らしてディテクタを検索します。

カテゴリ（Category）

検出するアプリケーションに割り当てられたカテゴリに照らしてディテクタを検索します。

タグ

検出するアプリケーションに割り当てられたタグに照らしてディテクタを検索します。

リスク（Risk）

検出するアプリケーションに割り当てられたリスク（Very High、High、Medium、Low、Very Low）を基準にディテクタを検索します。

ビジネスとの関連性（Business Relevance）

検出するアプリケーションに割り当てられたビジネスとの関連性（[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、[非常に低い（Very Low）]）に照らしてディテクタを検索します。

他のディテクタ ページへの移動

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 次のページを表示するには、**Right Arrow** ( )をクリックします。

ステップ 3 前のページを表示するには、**Left Arrow** ( )をクリックします。

ステップ 4 別のページを表示するには、ページ番号を入力して、Enter キーを押します。

ステップ 5 最後のページに移動するには、**Right End Arrow** ( )をクリックします。

ステップ 6 最初のページに移動するには、**Left End Arrow** ( )をクリックします。

ディテクタのアクティブおよび非アクティブの設定

ネットワークトラフィックを分析するためにディテクタを使用できるようにするには、その前に、ディテクタをアクティブにする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。

システムの検出機能を補完するために、ポートごとに複数のアプリケーションディテクタをアクティブにすることができます。

ポリシーのアクセス コントロール ルールにアプリケーションを含め、そのポリシーを導入するときに、そのアプリケーションに対してアクティブなディテクタがない場合、1つ以上のディ

テクタが自動的にアクティブになります。同様に、導入されているポリシーのアプリケーションが使用されているときに、そのアプリケーションのアクティブなディテクタをすべて非アクティブにしようとしても、ディテクタを非アクティブにすることはできません。

ヒント パフォーマンスを向上させるために、使用する予定のないアプリケーションプロトコル、クライアント、または Web アプリケーションのディテクタはすべて非アクティブにします。

注意 システムまたはカスタムのアプリケーション ディテクタをアクティブ化/非アクティブ化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 アクティブまたは非アクティブにするディテクタ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。

（注）
一部のアプリケーションディテクタはその他のディテクタによって必要とされることに注意してください。そのようなディテクタのいずれかを非アクティブにすると、それに依存するディテクタも無効となることを示す警告が表示されます。

カスタム アプリケーション ディテクタの編集

カスタム アプリケーション ディテクタを変更するには、次の手順を使用します。

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 変更するディテクタの横にある**Edit** ( )をクリックします。 代わりに **View** ( ) 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 3 カスタム アプリケーション ディテクタの設定 （13 ページ）の説明に従って、ディテクタを変更します。

ステップ 4 ディテクタの状態に応じて、次の保存オプションがあります。

- 非アクティブなディテクタを保存するには、[保存（Save）] をクリックします。
- 非アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。
- アクティブなディテクタを保存してすぐに使用を開始するには、[保存して再アクティブ化（Save and Reactivate）] をクリックします。

  注意
  カスタム アプリケーション ディテクタを保存して再びアクティブ化すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

- アクティブなディテクタを新規の非アクティブなディテクタとして保存するには、[新規保存（Save as New）] をクリックします。

ディテクタの削除

カスタムディテクタおよびCisco Professionalサービスが提供する個別にインポートされたアドオンディテクタを削除することができます。その他のCiscoが提供するディテクタを削除することはできませんが、その多くを非アクティブにすることはできます。

（注） ディテクタが展開されたポリシーで使用されている間は、そのディテクタを削除できません。

注意 アクティブ化されたカスタム アプリケーション ディテクタを削除すると、展開プロセスを経由することなく、ただちにSnortプロセスが再起動します。Snortプロセスの再起動を続行することが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内のいずれかの管理対象デバイスで発生します。 この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 **Policies** > **Application Detectors** を選択します。

ステップ 2 削除するディテクタの横にある **Delete** ( ) をクリックします。 代わりに **View** ( ) 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 3 **[OK]** をクリックします。

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。