発信トラフィックでの既存の感染のスキャン

この章で説明する内容は、次のとおりです。

発信トラフィックのスキャンの概要

悪意のあるデータがネットワークから発信されないようにするため、 Secure Web Applianceには発信マルウェアスキャン機能があります。ポリシー グループを使用して、マルウェアのスキャン対象となるアップロード、スキャンに使用するマルウェア対策スキャン エンジン、ブロックするマルウェアのタイプを定義できます。

Cisco Dynamic Vectoring and Streaming（DVS）エンジンは、トランザクション要求がネットワークから発信されるときにそれをスキャンします。Cisco DVS エンジンとの連携により、 Secure Web Applianceでは無意識のうちに悪意のあるデータがアップロードされるのを防止できます。

次の作業を実行できます。

タスク	タスクへのリンク
マルウェアをブロックするポリシーを作成する	アウトバウンド マルウェア スキャン ポリシーの設定 （3 ページ）
発信マルウェア ポリシー グループにアップロード要求を割り当てる	アップロード要求の制御 （6 ページ）

要求がDVSエンジンによってブロックされた場合のユーザーエクスペリエンス

Cisco DVS エンジンがアップロード要求をブロックすると、Web プロキシはエンド ユーザーにブロック ページを送信します。ただし、すべての Web サイトでエンド ユーザーにブロック ページが表示されるわけではありません。一部の Web 2.0 Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザーは適切にブロックされているので悪意のあるデータをアップロードすることはありませんが、そのことが Web サイトから通知されない場合もあります。

アップロード要求について

発信マルウェア スキャン ポリシーは、サーバーにデータをアップロードするトランザクション（アップロード要求）に対して、Web プロキシが HTTP 要求と復号化 HTTPS 接続をブロックするかどうかを定義します。アップロード要求は、要求本文にコンテンツが含まれている HTTP または復号化 HTTPS 要求です。

アップロード要求を受信すると、Web プロキシは要求を発信マルウェア スキャン ポリシー グループと比較して、適用するポリシー グループを決定します。ポリシー グループに要求を割り当てた後、ポリシー グループの設定済み制御設定と要求を比較し、要求をモニターするかブロックするかを決定します。発信マルウェア スキャン ポリシーによる判定で要求をモニターすることが決定されると、要求はアクセス ポリシーに対して評価され、Web プロキシが実行する最終アクションが該当するアクセス ポリシーによって決定されます。

（注） サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、発信マルウェア スキャン ポリシーに対して評価されません。

グループ メンバーシップの基準

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの以下の要素が考慮されます。

基準	説明
識別プロファイル（Identification Profile）	各クライアント要求は、**識別プロファイル**に一致するか、認証に失敗するか、ゲスト アクセスが許可されるか、または認証に失敗して終了します。

基準	説明
権限を持つユーザー	割り当てられた**識別プロファイル**が認証を必要とする場合に、そのユーザーが発信マルウェア スキャン ポリシー グループの承認済みユーザーのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、**識別プロファイル**がゲスト アクセスを許可している場合はゲスト ユーザーを指定できます。
詳細オプション（**Advanced options**）	発信マルウェア スキャン ポリシー グループ メンバーシップの複数の高度なオプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、**識別プロファイル**内に定義することもできます。高度なオプションを**識別プロファイル**内で設定すると、発信マルウェア スキャン ポリシー グループ レベルでは設定できなくなります。

クライアント要求と発信マルウェア スキャン ポリシー グループの照合

Web プロキシは、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その以下のポリシー グループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Web プロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

アウトバウンド マルウェア スキャン ポリシーの設定

宛先サイトの 1 つ以上のアイデンティティや URL カテゴリなど、複数の条件の組み合わせに基づいてアウトバウンド マルウェア スキャン ポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された ID の 1 つのみと一致する必要があります。

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 ポリシー グループの名前と説明（任意）を入力します。

（注） 各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4 [上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内のポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。

ステップ 5 [識別プロファイルおよびユーザー（Identification Profiles And Users）] セクションで、このポリシー グループに適用する 1 つまたは複数の ID グループを選択します。

ステップ 6 （任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

ステップ 7 いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）] は、このオプションの上に一覧表示されていないプロトコルを意味します。 （注） HTTPS プロキシをイネーブルにすると、復号化ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、アウトバウンド マルウェア スキャン、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。
プロキシ ポート（Proxy Ports）	Web プロキシへのアクセスに使用するプロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。 クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 （注） このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。

<table>
<tr><th>高度なオプション</th><th>説明</th></tr>
<tr><td>サブネット（Subnets）</td><td>サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。

関連 ID で定義されている可能性のあるアドレスを使用するか、またはここで特定のアドレスを入力することができます。

（注）　ポリシー グループに関連付けられている ID がアドレスによってメンバーシップを定義している場合は、ID で定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。</td></tr>
<tr><td>URL カテゴリ（URL Categories）</td><td>URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。

（注）　このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。</td></tr>
<tr><td>ユーザー エージェント（User Agents）</td><td>クライアント要求で使用されるユーザー エージェント（アップデータや Web ブラウザなどのクライアント アプリケーション）ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。

（注）　このポリシー グループに関連付けられている識別プロファイルが、この詳細設定によって識別プロファイル メンバーシップを定義している場合、非識別プロファイル ポリシー グループ レベルではこの設定項目を設定できません。</td></tr>
<tr><td>ユーザーの場所（User Location）</td><td>ユーザーのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。</td></tr>
</table>

ステップ 8　変更を送信します。

ステップ 9　アウトバウンド マルウェア スキャン ポリシー グループの管理を設定して、Web プロキシがトランザクションを処理する方法を定義します。

新しいアウトバウンド マルウェア スキャン ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

アップロード要求の制御

各アップロード要求は、アウトバウンドマルウェア スキャン ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。Webプロキシは、アップロード要求ヘッダーを受信することにより、要求本文をスキャンする必要があるかどうかを判定するための必要情報を得ます。DVS エンジンは要求をスキャンし、Web プロキシに判定を返します。必要に応じて、エンド ユーザーにブロック ページが表示されます。

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2 [接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3 [接続先設定の編集（Edit Destination Settings section）] セクションで、ドロップダウン メニューから [接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4 [スキャンする接続先（Destination to Scan）] セクションで、以下のいずれかを選択します。

オプション	説明
どのアップロードもスキャンしない（Do not scan any uploads）	DVSエンジンはアップロード要求をスキャンしません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
すべてのアップロードをスキャンする（Scan all uploads）	DVS エンジンはすべてのアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。
指定したカスタム URL カテゴリへのアップロードをスキャン（Scan uploads to specified custom URL categories）	DVS エンジンは、特定のカスタム URL カテゴリに属するアップロード要求をスキャンします。DVSエンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。 [カスタムカテゴリリストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

ステップ 5 変更を送信します。

ステップ 6 [マルウェア対策フィルタリング（Anti-Malware Filtering）] 列で、ポリシー グループのリンクをクリックします。

ステップ 7 [マルウェア対策設定（Anti-Malware Settings）] セクションで、[マルウェア対策カスタム設定の定義（Define Anti-Malware Custom Settings）] を選択します。

ステップ 8 [Cisco DVS マルウェア対策設定（Cisco DVS Anti-Malware Settings）] セクションで、このポリシー グループに対してイネーブルにするマルウェア対策スキャン エンジンを選択します。

ステップ 9 [マルウェア カテゴリ（Malware Categories）] セクションで、さまざまなマルウェア カテゴリをモニターするかブロックするかを選択します。

このセクションに一覧表示されるカテゴリは、イネーブルにするスキャンエンジンによって異なります。

（注） 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

DVS スキャンのロギング

アクセス ログは、DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを示します。各アクセス ログ エントリのスキャン判定情報セクションには、スキャンされたアップロードに対する DVS エンジン アクティビティの値が含まれています。フィールドのいずれかを W3C またはアクセス ログに追加すると、この DVS エンジン アクティビティをより簡単に検索できます。

表 *1 : W3C* ログのログ フィールドおよびアクセス ログのフォーマット指定子

W3C ログ フィールド	アクセス ログのフォーマット指定子
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアのアップロードをブロックするように設定されている場合、アクセス ログの ACL デシジョン タグは BLOCK_AMW_REQ になります。

ただし、DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアをモニターするように設定されている場合、アクセス ログの ACL デシジョン タグは、実際にトランザクションに適用されるアクセス ポリシーによって決まります。

DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを判断するには、各アクセス ログ エントリのスキャン判定情報セクションで、DVS エンジン アクティビティの結果を確認します。

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。