DNS ポリシー

ライセンス：任意

DNS ベースのセキュリティ インテリジェンスにより、クライアントが要求したドメイン名に基づいてトラフィックをブロックしたり、ブロック対象から除外したりできます。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタム リストやフィードを設定することも可能です。DNS ベースのセキュリティ インテリジェンスによるフィルタリングが実行されるタイミングは、ハードウェア レベルの処理およびトラフィックの復号が行われた後で、かつ、他のほとんどのポリシー ベースのインスペクション、分析、トラフィック処理が行われる前です。

DNS ポリシーによってブロックされたトラフィックは直ちにブロックされるため、他の詳細なインスペクション（侵入、エクスプロイト、マルウェアの有無など）の対象にはなりません。ブロックなしリストに追加することでブロックをオーバーライドしてアクセス制御ルールの評価を適用することができます。また、「モニタのみ」の設定をセキュリティ インテリジェンス フィルタリングに使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされた可能性がある接続を ASA FirePOWER モジュールが分析できるだけでなく、ブロックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

DNS ポリシーと、関連する DNS ルールを使用して、DNS ベースのセキュリティ インテリジェンスを設定します。展開するには、DNS ポリシーとアクセス コントロール ポリシーとを関連付け、次に設定を展開する必要があります。

- DNS ポリシーの構成要素 （1 ページ）
- DNS ルール （3 ページ）
- DNS ポリシーの導入 （10 ページ）

DNS ポリシーの構成要素

ライセンス：任意

DNS ポリシーを使用すると、ドメイン名ベースの接続をブロック（またはブロックから除外）できます。以下のリストでは、DNS ポリシーの作成後に変更できる設定を説明しています。

名前と説明

各 DNS ポリシーには一意の名前が必要です。説明は任意です。

ルール

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理するための詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。

DNS ポリシーを作成すると、ASA FirePOWER モジュールはそのポリシーをデフォルトのグローバル DNS ブロックなしリストのルールとデフォルトのグローバル DNS ブロックリストのルールに入力します。各ルールは、それぞれのカテゴリで先頭の位置に固定されます。ルールは変更できませんが、無効にすることはできます。モジュールはルールを、以下の順序で評価します。

- グローバル DNS ブロックなしリストのルール（有効になっている場合）
- ブロックなしのルール
- Global DNS ブロックのルール（有効になっている場合）
- ブロックとモニタのルール

通常、モジュールはドメイン名ベースのネットワーク トラフィックを、すべてのルールの条件がトラフィックと一致する最初の DNS ルールに従って処理します。トラフィックと一致する DNS ルールがない場合、モジュールは、関連するアクセス コントロール ポリシーのルールに基づいてトラフィックの評価を続行します。DNS ルールの条件は、単純なものにも複雑なものにもできます。

DNS ポリシーの編集

ライセンス：Protection

DNS ポリシーを同時に編集できるのは 1 ユーザのみであり、使用できるのは単一のブラウザ ウィンドウのみです。複数のユーザが同じポリシーを保存しようとすると、最初に保存された変更のセットのみが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで活動が行われずに 30 分が経過すると、警告が表示されます。60 分経過すると、モジュールは変更内容を破棄します。

DNS ポリシーを編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 DNS ポリシーを次のように編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[Rules] タブをクリックして、DNS ルールの作成と編集 （4 ページ）の説明に従って続行します。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

DNS ルール

ライセンス：任意

DNS ルールは、ホストにより要求されるドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価はすべてのトラフィック復号の後、およびアクセス コントロールの評価の前に実行されます。

ASA FirePOWER モジュールは、ユーザが指定した順序で DNS ルールをトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールの作成時に、モジュールはブロックなしのルールをモニタのルールやブロックのルールよりも前に配置し、最初にブロックなしのルールと照合してトラフィックを評価します。

.

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。DNS ルールは、DNS フィードまたはリスト条件が含まれていなければならず、セキュリティ ゾーンまたはネットワークを基準にしてトラフィックと突き合わせることもできます。

アクション

ルールのアクションによって、ASA FirePOWER モジュールによる一致するトラフィックの処理方法が決まります。

- ブロックなしリストにあるトラフィックが許可され、さらにアクセス制御インスペクションを受けます。
- モニタされるトラフィックは、残りのDNSブロックのルールによりさらに評価されます。トラフィックが DNS ブロックのルールに一致しない場合、アクセス制御ルールによりインスペクションを受けます。モジュールは、トラフィックのセキュリティインテリジェンス イベントをログに記録します。
- ブロックされたトラフィックは、それ以上のインスペクションは行われずにドロップされます。[Domain Not Found] 応答を返したり、DNS クエリをシンクホール サーバにリダイレクトしたりすることもできます。

DNS ルールの作成と編集

ライセンス：Protection

DNS ポリシーで、合計で最大 32,767 の DNS リストをブロックなしリストとブロックリストのルールに追加できます。つまり、DNS ポリシーのリスト数は、32767 より多くすることはできません。

DNS ルールを作成または編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 次の選択肢があります。

- 新しいルールを追加するには、[Add DNS Rule] をクリックします。
- 既存のルールを編集するには、編集アイコンをクリックします。

ステップ 3 [Name] を入力します。

ステップ 4 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [Action]：ルールのアクションを選択します。DNS ルールのアクション （6 ページ）を参照してください。
- [Conditions]：ルールの条件を設定します。DNS ルールの条件 （7 ページ）を参照してください。
- [Enabled]：ルールを有効にするかどうかを指定します。

ステップ 5 [追加（Add）] または [OK] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

DNS ルールの管理

ライセンス：任意

DNS ポリシー エディタの [Rules] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。他のアイコンには、警告、エラー、その他の重要な情報が表示されます。無効なルールは淡色表示され、ルール名の下に [（disabled）] というマークが付きます。

DNS ルールの有効化と無効化

ライセンス：Protection

作成した DNS ルールは、デフォルトでイネーブルになっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNS ポリシーのルール リストを表示すると、無効なルールは淡色表示されますが、変更は可能です。DNS ルール エディタを使用して DNS ルールをイネーブルまたはディセーブルにできることにも注意してください。

DNS ルールのイネーブル化とディセーブル化の方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 有効化または無効化するルールを含む DNS ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

ステップ 3 [OK] をクリックします。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

DNS ルールの評価順序

ライセンス：任意

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタ ルールの場合、モジュールはトラフィックをログに記録し、優先度が低い DNS ブロックリストのルールと照合してトラフィックの評価を続行します。
- 非モニタ ルールの場合、トラフィックがルールに一致したら、モジュールは追加の優先度が低い DNS ルールに突き合わせた評価を続行しません。

ルールの順序に関して、次の点に注意してください。

- グローバルブロックなしリストは常に最初に使用され、他のすべてのルールに優先します。
- [Do-Not-Block] セクションは [Block] セクションに優先します。ブロックなしのルールは常に他のルールに優先します。
- グローバルブロックリストは[Blocklist] セクション内で常に最初に使用され、他のすべてのモニタのルールやブロックリストのルールに優先します。
- [Blocklist] セクションには、モニタのルールとブロックリストのルールが含まれます。
- DNS ルールの最初の作成時に、モジュールはそれを、**[Do-Not-Block]** のアクションを割り当てる場合には [Do-Not-Block] セクションの末尾に配置し、その他のアクションを割り当てる場合は [Block] セクションの末尾に配置します。

それらを並べ替えて評価順序を変更するルールをドラッグ アンド ドロップできます。

DNS ルールのアクション

ライセンス：任意

すべての DNS ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：第一に、ルールアクションはルールの条件に一致するトラフィックをモジュールがモニタするか、またはブロックするか、あるいは処理の次段階に渡すことを許可するかを制御します。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

インライン展開されたデバイスのみがトラフィックをブロックできることに留意してください。パッシブに展開されたデバイスは、トラフィックの受け渡しやロギングはできますが、影響を与えることはありません。

ブロックなしのアクション

[Do-Not-Block] のアクションにより、一致するトラフィックの通過が許可されます。このオプションを選択した場合は、一致するアクセス制御ルール、またはアクセス コントロール ポリシーのデフォルトアクションのいずれかによって、トラフィックはさらにインスペクションを受けます。

モジュールはブロックなしの一致をログに記録しません。これらの接続のロギングは、その接続の最終的な傾向によって異なります。

モニタ アクション

[Monitor] のアクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックが直ちに受け渡されるか、またはブロックされることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。一致する最初の非モ

ニタ DNS ルールにより、モジュールがトラフィックをブロックするかどうかが決まります。追加の一致ルールがない場合、トラフィックはアクセス コントロール評価に従います。

DNS ポリシーによってモニタされる接続の場合、ASA FirePOWER モジュールは、接続終了セキュリティ インテリジェンス イベントと接続イベントをログに記録します。

ブロックのアクション

これらのアクションは、どんな種類のインスペクションもなく、トラフィックをブロックします。

- [Drop] アクションはトラフィックをドロップします。
- [Domain Not Found] アクションは、存在しないインターネット ドメイン応答を DNS クエリに返します。これによりクライアントは DNS 要求を解決できなくなります。
- [Sinkhole] アクションは、シンクホール オブジェクトの IPv4 または IPv6 アドレスを DNS クエリに応答して返します。シンクホール サーバは、IP アドレスへの後続の接続をログに記録するか、ログに記録してブロックすることができます。[Sinkhole] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[Drop] または **[Domain Not Found]** のアクションに基づいてブロックされた接続の場合は、モジュールが接続開始のセキュリティ インテリジェンス イベントと接続イベントをログに記録します。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続終了イベントはありません。

[Sinkhole] のアクションに基づいてブロックされる接続の場合、ロギングはシンクホールオブジェクトの設定に応じて決まります。シンクホール オブジェクトを、シンクホール接続のログ記録のみを実行するように設定した場合、モジュールは後続の接続の「接続の終わり」接続イベントをログに記録します。シンクホール オブジェクトを、シンクホール接続のログ記録およびブロックを実行するように設定した場合、モジュールは後続の接続の「接続の開始」接続イベントをログに記録し、それから接続をブロックします。

DNS ルールの条件

ライセンス：任意

DNS ルールの条件は、ルールで処理するトラフィックのタイプを特定します。条件は単純なものにも複雑なものにもできます。DNS フィードまたはリスト条件を定義する必要があります。セキュリティ ゾーンまたはネットワークでトラフィックをさらに制御できます。

条件を DNS ルールに追加するには、以下の手順に従います。

- ルールに対し特定の条件を設定しない場合、モジュールはその基準に基づいてトラフィックを照合しません。
- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。

- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、最大で 50 DNS のリストとフィードに基づいてトラフィックをブロックする単一のルールを使用できます。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

ライセンス：Protection

DNS ルールでゾーン条件を設定すると、トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、モジュールが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

DNS とセキュリティ ゾーンに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[Zones] タブをクリックします。

ステップ 2 [Available Zones] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 セキュリティ ゾーンをクリックするか、または右クリックして、[Select All] を選択します。

ステップ 4 [Add to Source] をクリックします。

ヒント 選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

DNS およびネットワークに基づくトラフィックの制御

ライセンス：Protection

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックの送信元 IP アドレスを明示的に指定できます。

DNS とネットワークに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[Networks] タブをクリックします。

ステップ 2 [Available Networks] から、次のように追加するネットワークを見つけて選択します。

- ネットワーク オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Networks] リストの上にある追加アイコンをクリックし、ネットワーク オブジェクトの操作の説明に従って続行します。
- 追加するネットワーク オブジェクトを検索するには、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Source] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4 手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[Source Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

ライセンス：Protection

DNS リスト、フィード、またはカテゴリにクライアントにより要求されたドメイン名が含まれる場合、DNS ルール内の DNS 条件によりトラフィックを制御できます。DNS ルール内で DNS 条件を定義する必要があります。

グローバルまたはカスタムのブロックなしリストまたはブラックリストを DNS 条件に追加するかどうかに関係なく、ASA FirePOWER モジュールは設定済みのルールアクションをトラフィックに適用します。たとえば、グローバルブロックなしリストをルールに追加し、[Drop] アクションを設定した場合、モジュールは追加のアセスメント用に渡されるはずだったすべてのトラフィックをブロックします。

DNS リスト、フィード、またはカテゴリに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[DNS] タブをクリックします。

ステップ 2 追加する DNS リストとフィードを、以下のように [DNS Lists and Feeds] から見つけて選択します。

- DNS リストまたはフィード（後で条件に追加可能）をその場で追加するには、[DNS Lists and Feeds] リストの上にある追加アイコンをクリックし、インテリジェンス フィードの操作の説明に従って続行します。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS Lists and Feeds] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオ

ブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Rule] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

DNS ポリシーの導入

ライセンス：任意

DNS ポリシー設定の更新が終了したら、変更を有効にするために、それをアクセス コントロール ポリシーの一部として展開する必要があります。次の手順を実行する必要があります。

- セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成の説明に従って、DNS ポリシーとアクセス コントロール ポリシーを関連付けます。
- 設定変更を展開します。設定変更の導入を参照してください。