DNS ポリシー

次のトピックでは、DNS ポリシー、DNS ルール、および DNS ポリシーを導入する方法について説明します。

DNS ポリシーの概要

ライセンス：任意（Any）

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、トラフィックをホワイトリスト/ブラックリストに登録できるようになります。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ラックリスト登録されたトラフィックは即座にブロックされるため、（侵入、エクスプロイト、マルウェアなどの）さらなるインスペクションの対象にはなりません。ブラックリストをホワイトリストで上書きしてアクセス コントロール ルールによる評価を強制することができます。また、セキュリティ インテリジェンス フィルタリングに「モニタ専用」設定を使用でき、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、ブラックリスト登録されたであろう接続を ASA FirePOWER モジュールが分析できるだけでなく、ブラ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 ポリシーおよび関連付けられた 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。これを展開するには、DNS ポリシーをアクセス コントロール ポリシーに関連付けた後、設定を展開する必要があります。

DNS ポリシーのコンポーネント

ライセンス:任意（Any）

DNS ポリシーにより、ドメイン名ベースの接続をホワイトリストまたはブラックリストに登録できるようになります。次のリストに、DNS ポリシーの作成後に変更可能な設定を示します。

名前（Name）と説明（Description）

各 DNS ポリシーには固有の名前が必要です。説明は任意です。

ルール（Rule）

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 モジュールはこれをデフォルトのグローバル DNS ホワイトリスト ルールおよびデフォルトのグローバル DNS ブラックリスト ルールに入力します。各ルールは、それぞれのカテゴリの先頭に固定されます。これらのルールは変更できませんが無効にすることはできます。ルールはモジュールにより次の順序で評価されます。

- グローバル DNS ホワイトリスト ルール（有効な場合）
- ホワイトリスト ルール
- グローバル DNS ブラックリスト ルール（有効な場合）
- ブラックリスト ルールおよびモニタ ルール

通常、モジュールによるドメイン名ベースのネットワーク 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。トラフィックに一致する DNS ルールがない場合、モジュールは、関連付けられたアクセス コントロール ポリシー ルールに基づいてトラフィックの評価を続行します。DNS ルール条件は単純または複雑のどちらでも構いません。

DNS ポリシーの編集

ライセンス: Protection

DNS ポリシーの編集は、1 つのブラウザ ウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存を試みた場合、最初に保存された一連の変更だけが保持されます。

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 30 分間操作が行われないと警告が表示されます。60 分後には、モジュールにより変更が破棄されます。

DNS ポリシーを編集する方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [DNS ポリシー（DNS Policy）] の順に選択します。

手順 2　DNS ポリシーを編集します。

- 名前（Name）と説明（Description）：名前または説明を変更するには、該当のフィールドをクリックし、新しい情報を入力します。
- ルール（Rules）：DNS ルールを追加、分類、有効化、無効化、または管理するには、[ルール（Rules）] タブをクリックし、DNS ルールの作成と編集（34-4 ページ）の説明に従って進みます。

手順 3　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-13 ページ）を参照してください。

DNS ルール

ライセンス：任意（Any）

DNS ルールは、ホストが要求す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、トラフィックの復号の後、アクセス コントロール評価の前に適用されます。

ASA FirePOWER モジュールは指定した順序で 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 ルールを作成すると、モジュールは、モニタ ルールとブラックリスト ルールの前にホワイトリスト ルールを配置し、最初にホワイトリスト ルールに対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（State）

デフォルトでは、ルールは有効になっています。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。

位置（Position）

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。モニタ ルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

条件（Conditions）

条件は、ルールが処理する特定のトラフィックを指定します。DNS ルールには、DNS フィードまたはリスト条件が含まれている必要があります。セキュリティ ゾーンまたはネットワークごとにトラフィックと照合することもできます。

アクション（Action）

ルールのアクションによって、一致するトラフィックを ASA FirePOWER モジュールがどのように処理するかが決まります。

- ホワイトリストに登録されたトラフィックは許可され、アクセス コントロールによるさらなるインスペクションの対象になります。

– モニタ対象のトラフィックは、残りの DNS ブラックリスト ルールにより、さらなる評価の対象となります。DNS ブラックリスト ルールに一致しないトラフィックは、アクセス コントロール ルールに検査されます。そのトラフィックのセキュリティ インテリジェンス イベントは、モジュールにより記録されます。

– ブラックリストに登録されたトラフィックは、追加のインスペクションなしでドロップされます。[検出されないドメイン（Domain Not Found）] 応答を返すか、シンクホール サーバに DNS クエリをリダイレクト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 ポリシーでは、ホワイトリスト ルールおよびブラックリスト ルールに最大で合計 32767 の DNS リストを追加できます。つまり、DNS ポリシー リストの数は 32767 を超えることができません。

DNS ルールを作成および編集する方法：

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [DNS ポリシー（DNS Policy）] の順に選択します。

手順 2　次の選択肢があります。

- 新しいルールを追加するには、[DNS ルールの追加（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。

手順 3　[名前（Name）] を入力します。

手順 4　以下のルール コンポーネントを設定するか、デフォルトを受け入れます。

- アクション（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（34-6 ページ）を参照してください。
- 条件（Conditions）：ルールの条件を設定します。DNS ルールの条件（34-7 ページ）を参照してください。
- 有効（Enabled）：ルールを**有効**にするかどうかを指定します。

手順 5　[追加（Add）] または [OK] をクリックします。

手順 6　[ASA FirePOWER の変更の保存（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（Any）

DNS ポリシー エディタの [ルール（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。他のアイコンにより、警告（ ）、エラー（ ）、その他の重要な情報（ ）が示されます。無効なルールはグレー表示され、ルール名の下に [無効（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、デフォルトで有効になっています。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、無効なルールはグレー表示されますが、変更は可能です。また、DNS ルール エディタを使用して DNS ルールを有効または無効にできることに注意してください。

DNS ルールを有効または無効にする方法：

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [DNS ポリシー（DNS Policy）] の順に選択します。

手順 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。

手順 3　[OK] をクリックします。

手順 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

次の作業

- 設定変更を展開します。設定変更の展開（4-13 ページ）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（Any）

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 ルールでは、モジュールはまずトラフィックを記録し、その後、優先順位の低い DNS ブラックリスト ルールに対してトラフィックを評価を続行します。
- モニタ ルール以外では、トラフィックがルールに一致した後、モジュールは優先順位の低い追加の DNS ルールに対してトラフィックの評価は続行しません。

ルールの順序については、以下の点い注意してください。

- グローバル ホワイトリストは常に先頭で、他のすべてのルールよりも優先されます。
- ホワイトリスト セクションはブラックリスト セクションよりも優先され、ホワイトリスト ルールは常に他のルールよりも優先されます。
- グローバル ブラックリストは常にブラックリスト セクションの先頭で、他のモニタ ルールおよびとブラックリスト ルールよりも優先されます。
- ブラックリスト セクションには、モニタ ルールおよびブラックリスト ルールが含まれます。
- 初めて DNS ルールを作成したときは、ホワイトリスト アクションを割り当てるとそれはモジュールによりホワイトリスト セクションの最後に配置され、他のアクションを割り当てるとブラックリスト セクションの最後に配置されます。

ルールをドラッグ アンド ドロップして順序を変えて、評価の順序を変更することができます。

DNS ルールのアクション

ライセンス:任意（Any）

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:まずルール アクションは、モジュールがルールの条件に一致するトラフィックをホワイトリスト登録、モニタ、またはブラックリスト登録するかどうかを制御します。
- 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。

インラインで展開されたデバイスのみがトラフィックをブラックリスト登録できることに留意してください。パッシブ展開されたデバイスは、トラフィックのホワイトリスト登録およびロギングはできますが、トラフィックに影響を与えることはできません。

[ホワイトリスト（Whitelist）] アクション

[ホワイトリスト（Whitelist）] 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。トラフィックをホワイトリスト登録すると、そのトラフィックは、照合するアクセス コントロール 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 アクションによるさらなるインスペクションの対象になります。

モジュールは、ホワイトリストの一致はロギングしません。ただし、ホワイトリストに登録された接続のロギングは、接続の最終的な傾向によって異なります。

[モニタ（Monitor）] アクション

[モニタ（Monitor）] 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ただちにホワイトリスト登録されたりブラックリスト登録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。モニタ ルール以外の一致する最初の DNS ルールが、モジュールがトラフィックをブラックリスト登録するかどうかを決定します。一致する追加のルールがなければ、トラフィックはアクセス コントロール評価の対象となります。

DNS ポリシーによってモニタされる接続については、ASA FirePOWER モジュールは、接続終了セキュリティ インテリジェンスと接続イベントをロギングします。

[ブラックリスト（Blacklist）] アクション

[ブラックリスト（Blacklist）] アクションは、いかなる種類のインスペクションなしで、トラフィックをブラックリスト登録します。

- [ドロップ（Drop）] アクションはトラフィックをドロップします。
- [検出されないドメイン（Domain Not Found）] アクションは、存在しないインターネット ドメインの応答を DNS クエリに返し、これによりクライアントが DNS 要求を解決することを防ぎます。
- [シンクホール（Sinkhole）] アクションは、応答内のシンクホール 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ギングするか、またはロギングしてブロックすることができます。[シンクホール（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。

[ドロップ（Drop）] または [検出されないドメイン（Domain Not Found）] アクションに基づいてブラックリスト登録された接続については、モジュールは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録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の終了イベントはありません。

[シンクホール（Sinkhole）] アクションに基づいてブラックリスト登録された接続については、ロギングはシンクホール オブジェクト設定によって異なります。シンクホール オブジェクトを、シンクホール接続をロギングのみするよう設定している場合、モジュールは、後続の接続の接続終了イベントをロギングします。シンクホール オブジェクトを、シンクホール接続をロギングしてブロックするよう設定している場合、モジュールは、後続の接続の接続開始イベントをロギングし、その後、その接続をブロックします。

DNS ルールの条件

ライセンス:任意（Any）

DNS ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑のどちらでも構いません。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によってトラフィックをさらに制御できます。

DNS ルールに条件を追加するときは、以下に留意してください。

- 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 の条件を追加できます。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、単一ルールを使用して、最大 50 の DNS リストおよびフィードに基づいてトラフィックをブラックリスト登録できます。

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 ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。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 およびセキュリティ ゾーンに基づいてトラフィックを制御する方法:

手順 1　DNS ルール エディタで、[ゾーン（Zones）] タブをクリックします。

手順 2　[利用可能なゾーン（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、[利用可能なゾーン（Available Zones）] リストの上にある [名前で検索（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。

手順 3　クリックして 1 つのゾーンを選択するか、右クリックして [すべて選択（Select All）] を選択します。

手順 4　[送信元に追加（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。

手順 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-13 ページ）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に対し、明示的に送信元 IP アドレスを指定できます。

DNS およびネットワークに基づいてトラフィックを制御する方法：

手順 1　DNS ルール エディタで、[ネットワーク（Networks）] タブをクリックします。

手順 2　[利用可能なネットワーク（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。

- ここでネットワーク オブジェクトを追加するには（後で条件に追加できます）、[利用可能なネットワーク（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（3-4 ページ）の説明に従って進みます。
- 追加するネットワーク オブジェクトを検索するには、[利用可能なネットワーク（Available Networks）] リストの上にある [名前または値で検索（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。

手順 3　[送信元に追加（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。

手順 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。[送信元ネットワーク（Source Networks）] リストの下にある [IP アドレスの入力（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 [追加（Add）] をクリックします。

手順 5　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開（4-13 ページ）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、またはカテゴリがクライアントから要求されたドメイン名を含む場合、DNS ルール内の DNS 条件によりトラフィックを制御することができます。DNS ルール内の 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ホワイト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わらず、ASA FirePOWER モジュールは設定されたルール アクションをトラフィックに適用します。たとえばルールにグローバル ホワイトリストを追加し、[ドロップ（Drop）] アクションを設定すると、モジュールはホワイトリスト登録されている必要があるすべてのトラフィックをブラックリスト登録します。

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:

手順 1　DNS ルール エディタで、[DNS] タブをクリックします。

手順 2　次のように、[DNS リストおよびフィード(DNS Lists and Feeds)] から追加する DNS リストおよびフィードを検索して選択します。

- ここで DNS リストまたはフィードを追加するには(後で条件に追加できます)、[DNS リストおよびフィード(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(3-7 ページ)の説明に従って進みます。
- 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 リストおよびフィード(DNS Lists and Feeds)] リストの上にある [名前または値で検索(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。

手順 3　[ルールに追加(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。

手順 4　ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。設定変更の展開(4-13 ページ)を参照してください。

DNS ポリシーの導入

ライセンス:任意(Any)

DNS ポリシー設定は、更新を終了した後、変更を有効にするためにアクセス コントロール ポリシーの一部として導入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ホワイトリストおよびブラックリストの作成(5-4 ページ)で説明されているように、DNS ポリシーをアクセス コントロール ポリシーに関連付けます。
- 設定変更を展開します。設定変更の展開(4-13 ページ)を参照してください。