DNS ポリシー

次のトピックでは、DNS ポリシーと DNS ルールについて、および管理対象デバイスに 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

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 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、他のさらなるインスペクションの対象にはなりません（侵入、エクスプロイト、マルウェアなどについてだけでなくネットワーク検出についても）。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システム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。

（注） 期限切れのため、またはクライアントの DNS キャッシュやローカル DNS サーバのキャッシュがクリアされているか、期限切れであるために、DNS サーバでドメイン キャッシュが削除されない場合に、DNS ベースのセキュリティ インテリジェンスが意図したとおりに機能しないことがあります。

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。デバイスにこれを展開するには、アクセス コントロール ポリシーに DNS ポリシーを関連付けてから管理対象デバイスに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

DNSポリシーにより、ドメイン名に基づいて、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。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

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。システムは、ルール番号の昇順で、トラフィックを DNS ルールと上から順に照合します。

DNS ポリシーを作成すると、システム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。両方のルールは、それぞれのカテゴリで先頭の位置に固定されます。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。

マルチドメイン展開では、子孫DNSホワイトリスト ルールおよび子孫DNSブラックリスト ルールも先祖ドメインの DNS ポリシーに追加されます。これらのルールは、それぞれのカテゴリの 2 番目の位置に固定されます。

（注） Firepower Management Center でマルチテナンシーが有効になっている場合、システムは先祖ドメインと子孫ドメインを含むドメインの階層に編成されます。これらのドメインは、DNS 管理で使用されるドメイン名とは別になります。

子孫のリストには、Firepower システムのサブドメイン ユーザによってホワイトリストまたはブラックリストに登録されたドメインが含まれます。先祖ドメインから、子孫のリストの内容を表示することはできません。サブドメイン ユーザをホワイトリストまたはブラックリストに登録しない場合は、次を実行します。

- 子孫のリストのルールを無効にします。
- アクセス コントロール ポリシーの継承設定を使用してセキュリティ インテリジェンスを適用します。

ルールはシステム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）
- 子孫 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）
- 子孫 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、システムによるDN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、システムは、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。

基本 DNS ポリシーの作成

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]**を選択します。

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

ステップ 3 [名前（Name）]に一意のポリシー名を入力し、オプションで[説明（Description）]にポリシーの説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 必要に応じて、セキュリティ インテリジェンスによる接続のロギングの説明に従って、さらに新しいポリシーを設定します。
- 設定変更を展開します。設定変更の展開を参照してください。

DNS ポリシーの編集

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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、システムにより変更が破棄されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [DNS]**を選択します。

ステップ 2 編集する DNS ポリシー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 3 DNS ポリシーを編集します。

- 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、[ルール（Rules）] タブをクリックして、DNS ルールの作成および編集 （7 ページ）の説明に従って続行します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

DNS ポリシーの管理

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

[DNS ポリシー（DNS Policy）]ページ（**[ポリシー（Policies）]** > **[アクセス コントロール（Access Control）]** > **[DNS]**）を使用して、DNS のカスタム ポリシーを管理します。自分で作成したカスタム ポリシーに加えて、システムにはデフォルトの DNS ポリシーが用意されています。このポリシーは、デフォルトのブラックリストとホワイトリストを使用します。このシステム付属のカスタム ポリシーは編集して使用できます。マルチドメイン展開では、このデフォルトポリシーはデフォルトのグローバル DNS ブラックリスト、グローバル DNS ホワイトリスト、子孫 DNS ブラックリスト、および子孫 DNS ホワイトリストを使用します。また、このポリシーはグローバル ドメインでのみ編集できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシー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）]** > **[アクセス コントロール（Access Control）]** > **[DNS]**を選択します。

ステップ 2 DNS ポリシーを以下のように管理します。

- 比較：DNS ポリシーを比較するには、[ポリシーの比較（Compare Policies）]をクリックして、ポリシーの比較で説明する手順を実行します。
- コピー：DNS ポリシーをコピーするには、コピー アイコン（）をクリックして、DNS ポリシーの編集 （4 ページ）で説明する手順を実行します。
- 作成：新しい DNS ポリシーを作成するには、[DNS ポリシーの追加（Add DNS Policy）]をクリックし、基本 DNS ポリシーの作成 （3 ページ）で説明する手順を実行します。
- 削除：DNS ポリシーを削除するには、削除アイコン（）をクリックし、ポリシーの削除を確認します。
- 編集：既存の DNS ポリシーを変更するには、編集アイコン（）をクリックし、DNS ポリシーの編集 （4 ページ）で説明する手順を実行します。

DNS ルール

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。

システムは指定した順序でトラフィックを DNS ルールと照合します。ほとんどの場合、システム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、システムは、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、システムはネットワーク 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。システムは、ルール番号の昇順で上から順に、トラフィックをルールと照合します。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、セキュリティゾーン、ネットワーク、または VLAN によってトラフィックと照合することができます。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。

- 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、システム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。

関連トピック

セキュリティ インテリジェンスについて

DNS ルールの作成および編集

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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 ルールに合計 32767 個まで DNS リストを追加できます。つまり、DNS ポリシーのリストの数が 32767 を超えることはできません。

手順

ステップ 1 DNS ポリシー エディタには、以下のオプションがあります。

- 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。

ステップ 2 [名前（Name）] を入力します。

ステップ 3 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（Action）] を選択します。DNS ルールのアクション （9 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 （11 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。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

DNS ルールの管理

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

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）
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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、システムはネットワーク 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。

手順

ステップ 1 DNS ポリシー エディタで、ルールを右クリックしてルール状態を選択します。

ステップ 2 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

DNS ルールの評価順序

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。システムは、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、システム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、システム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の評価を続行します。
- 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、システム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。
- 子孫 DNS ホワイトリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常に2番目であり、グローバル ホワイトリストを除き、他のすべて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。
- 子孫 DNS ブラックリスト ルールは、マルチドメイン展開の非リーフ ドメインでのみ表示されます。これは常にブラックリスト セクションの 2 番目であり、グローバル ブラックリストを除き、他のすべてのモニタ ルールおよびブラックリスト 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システム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、これらの順序を変更できます。

DNS ルールのアクション

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、システム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。パッシブに展開されたデバイスまたはタップ モードで展開されたデバイスは、トラフィックをホワイトリスト登録およびロギングできますが、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。

システムは、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、システム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、システムは、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 Firepower Management Center データベースにロギングします。

[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、システム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、システムは、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、システムは、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。

（注） ASA FirePOWER デバイスでシンクホール アクションを使用して DNS ルールを設定し、トラフィックがルールに一致する場合、デフォルトでは ASA によって、後続のシンクホール接続がブロックされます。回避策として、ASA コマンド ラインから次のコマンドを実行します。

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

ASA が引き続き接続をブロックする場合は、サポートにお問い合わせください。

関連トピック

ログ可能なその他の接続

DNS ルールの条件

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 ルール内の 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。また、必要に応じてセキュリティ ゾーン、ネットワーク、または VLAN によってトラフィックを制御できます。

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、システム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。たとえば、DNS フィードまたはリスト条件およびネットワーク条件を含み、VLAN タグ条件を含まないルールは、セッション中の VLAN タグに関係なく、ドメイン名と送信元または宛先に基づいてトラフィックを評価します。
- 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

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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、複数のデバイス間に配置されている場合がある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、システム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。

手順

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

ステップ 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。

ステップ 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。

ステップ 4 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

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。設定変更の展開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

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）
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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。

手順

ステップ 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。

ステップ 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 オブジェクトの作成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、オブジェクトのいずれかのコンポーネント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 [送信元に追加（Add to Source）] をクリックするか、ドラッグ アンド ドロップします。

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。[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。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

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。設定変更の展開を参照してください。

DNS および VLAN に基づくトラフィックの制御

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

DNS ルールで VLAN 条件を設定すると、トラフィックの VLAN タグに応じてそのトラフィックを制御できます。システムは、最も内側の VLAN タグを使用して VLAN を基準にパケットを識別します。

VLAN ベースの DNS ルール条件を作成するときは、VLAN タグを手動で指定できます。または、VLAN タグ オブジェクトを使用して VLAN 条件を設定することもできます。VLAN タグ オブジェクトとは、いくつかの VLAN タグに名前を付けて再利用可能にしたものを指します。

手順

ステップ 1 DNS ルール エディタで、[VLAN タグ（VLAN Tags）] タブを選択します。

ステップ 2 [利用可能な VLAN タグ（Available VLAN Tags）] で、追加する VLAN を選択します。

- VLAN タグ オブジェクトをここで追加するには（後で条件に追加できます）、[利用可能な VLAN タグ（Available VLAN Tags）] リストの上にある追加アイコン（）をクリックし、VLAN タグ オブジェクトの作成の説明に従って進みます。
- 追加する VLAN タグ オブジェクトおよびグループを検索するには、[利用可能な VLAN タグ（Available VLAN Tags）] 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、オブジェクト名またはオブジェクトの VLAN タグの値を入力します。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 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 4 手動で指定する VLAN タグを追加します。[選択した VLAN タグ（Selected VLAN Tags）] リストの下にある [VLAN タグの入力（Enter a VLAN Tag）] プロンプトをクリックし、VLAN タグまたはその範囲を入力して、[追加（Add）] をクリックします。1 から 4094 までの任意の VLAN タグを指定できます。VLAN タグの範囲を指定するにはハイフンを使用します。

システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の VLAN タグを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

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。設定変更の展開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

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
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

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、システム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、システム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。

手順

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 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。

- DNS リストまたはフィードをここで追加するには（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、セキュリティ インテリジェンス フィードの作成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。

ステップ 3 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

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。設定変更の展開を参照してください。

DNS ポリシーの展開

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
脅威	保護	任意（Any）	任意（Any）

DNS のポリシー設定の更新を終了した後に、アクセス コントロール設定の一部としてこれを展開する必要があります。

- セキュリティ インテリジェンスの設定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。設定変更の展開を参照してください。