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、セキュリティ インテリジェンス ブロックリストを使用して、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 ポリシーのブロックリストに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）。セキュリティ インテリジェンス ブロックしないリストを使用してブロックリストより優先させて、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「モニター専用」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、ブロックリストによってブロック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。

（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 サーバー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 サーバーでドメイン 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。

Cisco Umbrella DNS ポリシー

管理センターの Cisco Umbrella DNS 接続は、DNS クエリを Cisco Umbrella にリダイレクトするのに役立ちます。これにより、Cisco Umbrella で要求を検証し、ドメイン名に基づき要求を許可またはブロックし、要求に DNS ベースのセキュリティポリシーを適用できます。Cisco Umbrella を使用する場合、Cisco Umbrella 接続を設定して（[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella接続（Cisco Umbrella Connection）]）DNS クエリを Cisco Umbrella へリダイレクトできます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。これにより、次の 2 系統の保護が可能になります。

- ローカル DNS インスペクションポリシー
- Cisco Umbrella のクラウドベースのポリシー

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

Management Center から Cisco Umbrella に DNS 要求をリダイレクトするには、次の手順を実行します。

1. Cisco Umbrella の接続設定を設定する
2. Cisco Umbrella DNS ポリシーを作成および設定します。
3. Cisco Umbrella 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。
4. 変更を展開します。

管理センターで Cisco Umbrella DNS Connector を設定する方法の詳細については、「Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定」を参照してください。

DNS ポリシーの構成要素

DNS ポリシーにより、ブロックリストを使用してドメイン名に基づいて接続をブロックしたり、ブロックしないリストを使用してそのような接続をこのタイプのブロックから除外したりできます。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。

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 DNS ルールのデフォルトのグローバルブロックしないリストおよび DNS ルールのデフォルトのグローバルブロックリストに入力します。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。

（注） 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、システムのサブドメインユーザーのブロックリストまたはブロックしないリストに載っている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ーがドメインをブロックリストまたはブロックしないリストに追加しないようにするには、次の手順を実行します。

- 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。

- DNS ルールのグローバル ブロックしないリスト（有効になっている場合）
- 子孫 DNS ブロックしないリストルール（有効な場合）
- [ブロックしない（Do Not Block）] アクションを使用したルール
- DNS ルールのグローバルブロックリスト（有効になっている場合）
- 子孫 DNS ブロックリストルール（有効な場合）

- [ブロックしない（Do Not Block）] 以外のアクションを使用したルール

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。

DNS ポリシーのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

DNS ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

重要 トラフィックの DNS 検証を成功させるには、デバイスにネットワーク検出ポリシーを適用する必要があります。

DNS および Cisco Umbrella DNS ポリシーの管理

[DNSポリシー（DNS Policy）] ページ（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[DNS]**）を使用して、DNS および Cisco Umbrella DNS のカスタムポリシーを管理します。

ユーザーが作成するカスタムポリシーに加えて、デフォルトの DNS ポリシーとデフォルトの Cisco Umbrella DNS ポリシーが用意されています。デフォルトの DNS ポリシーでは、デフォルトのブロックリストとブロックしないリストが使用されます。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。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（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（Copy）]（）をクリックして、DNS ポリシーの編集 （6 ページ）で説明する手順を実行します。
- 作成：新しい Cisco Umbrella DNS ポリシーを作成するには、**[新しいポリシー（New Policy）]** > **[Cisco Umbrella DNSポリシー（Umbrella DNS Policy）]**をクリックし、Cisco Umbrella DNS ポリシーを作成する （21 ページ）の説明に従って続行します。
- 削除：DNS または Cisco Umbrella DNS ポリシーを削除するには、[削除（Delete）]（）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（Edit）]**（）をクリックし、DNS ポリシーの編集 （6 ページ）で説明する手順を実行します。既存の Cisco Umbrella DNS ポリシーを変更するには、**[編集（Edit）]**（）をクリックし、Cisco Umbrella DNS ポリシーとルールの編集 （21 ページ）の説明に従って続行します。

基本的な DNS ポリシーの作成

新しい DNS ポリシーを作成した場合、デフォルト設定が含まれています。その後、ポリシーを編集して動作をカスタマイズする必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（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）]** > **[DNSポリシー（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

ポリシーを設定します。DNS ポリシーの編集 （6 ページ） を参照してください。

DNS ポリシーの編集

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。複数のユーザー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）] > [アクセス制御（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（Edit）]**（）をクリックします。

代わりに [表示（View）]（） 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）] をクリックして、DNS ルールの作成と編集 （8 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

- 必要に応じて、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*Logging Connections with Security Intelligence*」の説明に従ってい新しいポリシーをさらに設定します。
- 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 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。

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、ルールを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（Whitelist）]>[ブロックしない（Do Not Block）] アクションの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。
- モニターされるトラフィックは、残りの DNS ブロックリストのルールによりさらに評価されます。トラフィックが DNS ブロックリストルールに一致しない場合、アクセスコントロールルールによりインスペクションを受けます。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。
- ブロックリストのトラフィックは、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。

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 ルールの作成と編集

DNS ポリシーでは、ブロックリストルールおよびブロックしない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（Edit）]**（ ） をクリックします。

ステップ 2 名前を入力します。

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 （10 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。その他のアイコンは、[警告（Warning）]（ ）、[エラー（Error）]（ ）、およびその他の重要[情報（Information）]（ ）を表します。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

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、トラフィックを DNS ルールと上から順に照合します。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。

- モニタールールでは、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 ブロ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。
- モニタールール以外では、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。

- DNS のグローバルブロックしない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。
- [ブロックしないリスト（Do-Not-Block List）] セクションは [ブロックリスト（Block List）] セクションに優先します。ブロックしないリストのルールは常に他のルールに優先します。
- DNS のグローバルブロックリストは [ブロックリスト（Block List）] 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ーのルールやブロックリストのルールに優先します。
- [ブロックリスト（Block List）] セクションには、モニターのルールとブロックリストのルールが含まれます。
- 初めて DNS ルールを作成したときは、[ブロックしない（Do Not Block）] アクションを割り当てるとそれはシステムにより [ブロックしないリスト（Do-Not-Block List）] 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 [ブロックリスト（Block List）] 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：第一に、ルールアクションは、ブロックリストまたはブロックしないリストに基づいて、システムがルールの条件に一致するトラフィックをブロックするか、ブロックしないか、またはモニター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。

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、Threat Intelligence Director-Management Center のアクションの優先順位付けを参照してください。

[ブロックしない（Do Not Block）] アクション

[ブロックしない（Do Not Block）] アクションでは、トラフィックは検査の次のフェーズであるアクセス制御ルールに渡されます。

システムは [ブロックしない（Do Not Block）] リスト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

[モニター（Monitor）] アクションは接続ロギングを強制するように設計されています。つまり、一致するトラフィックが即時に許可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。モニター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ロック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ー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 Management Center データベースにロギングします。

ブロック 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。

- [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（A および AAAA レコードのみ）。シンクホール サーバーは、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）] のアクションに基づいてブロックされた接続の場合は、システム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。

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、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。

関連トピック

セキュリティゾーンルール条件 （12 ページ）
ネットワークルール条件
VLAN タグルール条件
DNS ルールの条件 （13 ページ）

セキュリティゾーンルール条件

セキュリティ ゾーンを利用すると、ネットワークをセグメント化し、複数のデバイスでインターフェイスをグループ化して、トラフィック フローを管理および分類する上で助けになります。

ゾーンのルール条件では、トラフィックをその送信元と宛先のセキュリティゾーンで制御します。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加すると、送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過するトラフィックだけが一致することになります。

ゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要があるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

ヒント ゾーンによってルールを制限することは、システムのパフォーマンスを向上させる最適な手段の 1 つです。ルールがデバイスのインターフェイスを通過するトラフィックに適用しなければ、ルールがそのデバイスのパフォーマンスに影響することはありません。

セキュリティ ゾーン条件とマルチテナンシー

マルチドメイン導入では、先祖ドメイン内に作成されるゾーンに、別のドメイン内にあるデバイス上のインターフェイスを含めることができます。子孫ドメイン内のゾーン条件を設定すると、その設定は表示可能なインターフェイスだけに適用されます。

ネットワークルール条件

ネットワーク ルールの条件では、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネル ルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

（注） アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

VLAN タグルール条件

（注） アクセスルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Threat Defense ：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

DNS ルールの条件

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ブロックリストまたはブロックしないリストを DNS 条件に追加するかどうかにかかわらず、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ブロックしないリストを追加し、[ドロップ（Drop）]アクションを設定すると、システムは検査の次のフェーズに渡すことが許可されている必要があるすべてのトラフィックをブロックします。

DNS ルールの作成方法

次のトピックでは、DNS ルールの作成方法について説明します。

関連トピック

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 （14 ページ）
DNS およびネットワークに基づくトラフィックの制御 （14 ページ）
DNS および VLAN に基づくトラフィックの制御 （15 ページ）
DNS リストまたはフィードに基づくトラフィックの制御 （16 ページ）

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

DNS ルール内のゾーン条件によって、その送信元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。

手順

ステップ 1 DNS ルールエディタで、[ゾーン（Zones）] 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

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）] 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。

- 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、[利用可能なネットワーク（Available Networks）] リストの上にある**Add** (＋)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、[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。

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

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）] 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**Add** (＋)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。

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 リストまたはフィードに基づくトラフィックの制御

手順

ステップ 1 DNS ルールエディタで、[DNS] 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（後で条件に追加可能）をその場で追加するには、[DNSリストおよびフィード（DNS Lists and Feeds）] リストの上にある **Add** ( ) 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 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。
- システム提供の脅威カテゴリの説明については、セキュリティ インテリジェンス カテゴリを参照してください。

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 ポリシーの導入

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。

Cisco Umbrella DNS ポリシー

管理センターの Cisco Umbrella DNS 接続は、DNS クエリを Cisco Umbrella にリダイレクトするのに役立ちます。これにより、Cisco Umbrella で要求を検証し、ドメイン名に基づき要求を許可またはブロックし、要求に DNS ベースのセキュリティポリシーを適用できます。Cisco Umbrella を使用する場合、Cisco Umbrella 接続を設定して（[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella接続（Cisco Umbrella Connection）]）DNS クエリを Cisco Umbrella へリダイレクトできます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシーマップにより、DNS インスペクションの設定に基づいて要求をブロックするか、または、要求をドロップすることに決定した場合、その要求は Cisco Umbrella へ転送されません。これにより、次の 2 系統の保護が可能になります。

- ローカル DNS インスペクションポリシー
- Cisco Umbrella のクラウドベースのポリシー

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張機能）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザー名と内部の IP アドレスのプライバシーを確保することもできます。

Management Center から Cisco Umbrella に DNS 要求をリダイレクトするには、次の手順を実行します。

1. Cisco Umbrella の接続設定を設定する
2. Cisco Umbrella DNS ポリシーを作成および設定します。
3. Cisco Umbrella 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。
4. 変更を展開します。

管理センターで Cisco Umbrella DNS Connector を設定する方法の詳細については、「Cisco Secure Firewall Management Center 向け Cisco Umbrella DNS Connector の設定」を参照してください。

DNS 要求を Cisco Umbrella にリダイレクトする方法

ここでは、Management Center を使用してデバイスから Cisco Umbrella に DNS 要求をリダイレクトする手順について説明します。

手順	操作手順	詳細
1	前提条件を満たしていることを確認する	Cisco Umbrella DNS コネクタを設定するための前提条件 （18 ページ）
2	Cisco Umbrella の接続設定を設定する	Cisco Umbrella の接続設定の設定 （19 ページ）
3	Cisco Umbrella DNS ポリシーを作成する	Cisco Umbrella DNS ポリシーを作成する （21 ページ）
4	Cisco Umbrella DNS ポリシーを設定する	Cisco Umbrella DNS ポリシーとルールの編集 （21 ページ）
5	Cisco Umbrella 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る	Cisco Umbrella 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る （22 ページ）

Cisco Umbrella DNS コネクタを設定するための前提条件

表 *1:* サポートされる最小プラットフォーム

製品	バージョン
Secure Firewall Threat Defense	6.6 以降
Secure Firewall Management Center	7.2 以降

- https://umbrella.cisco.com で Cisco Umbrella のアカウントを確立し、http://login.umbrella.com で Umbrella にログインします。
- Cisco Umbrella サーバーから Management Center に CA 証明書をインポートします。Cisco Umbrella で、[展開（Deployments）] > [構成（Configuration）] > [ルート証明書（Root Certificate）] を選択し、証明書をダウンロードします。

  Cisco Umbrella 登録サーバーとの間で HTTPS 接続を確立するために、ルート証明書をインポートする必要があります。証明書は、SSL サーバー検証のために信頼される必要があります。これは、Management Center ではデフォルトのオプションではありません。Management Center でデバイスの以下の証明書をコピーして貼り付けます（[デバイス（Device）] > [証明書（Certificates）]）。

```
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
```

Management Center に証明書を追加する場合は、[CAのみ（CA Only）] チェックボックスをオンにします。

- デバイスに証明書をインストールします。
- Cisco Umbrella から次のデータを取得します。
  - 組織 ID
  - ネットワークデバイスキー
  - ネットワーク デバイス シークレット
  - レガシー ネットワーク デバイス トークン
- Management Center がインターネットに接続していることを確認します。
- Management Center で、輸出規制機能オプションのある基本ライセンスが有効になっていることを確認します。
- api.opendns.com を解決するように DNS サーバーが設定されていることを確認します。
- Management Center がポリシー構成の management.api.umbrella.com を解決できることを確認します。
- api.opendns.com への Threat Defense ルートを設定します。

Cisco Umbrella の接続設定の設定

Cisco Umbrella の接続設定では、Cisco Umbrella にデバイスを登録するために必要なトークンを定義します。

始める前に

Cisco Umbrella https://umbrella.cisco.com でアカウントを確立し、https://dashboard.umbrella.com で Cisco Umbrella にログインし、Cisco Umbrella への接続を確立するために必要な情報を取得します。

手順

ステップ 1 **[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella接続（Cisco Umbrella Connection）]**を選択します。

ステップ 2 次の詳細を取得し、[一般（General）] 設定に追加します。

- [組織ID（Organization ID）]：Cisco Umbrella で組織を識別する一意の番号。すべての Umbrella 組織は、Umbrella の個別のインスタンスであり、独自のダッシュボードを持ちます。組織は名前と組織 ID によって識別されます。
- [ネットワークデバイスキー（Network Device Key）]：Cisco Umbrella から Umbrella ポリシーを取得するためのキー。
- [ネットワークデバイスシークレット（Network Device Secret）]：Cisco Umbrella から Umbrella ポリシーを取得するためのシークレット。
- [レガシーネットワークデバイストークン（Legacy Network Device Token）]：Cisco Umbrella レガシー ネットワーク デバイス API トークンは、Cisco Umbrella ダッシュボードを通じて発行されます。Cisco Umbrella では、ネットワークデバイスを登録するために API トークンが必要です。

ステップ 3 [詳細設定（Advanced）] から次のオプションを設定できます。

- [DNSCrypt公開キー（DNSCrypt Public Key）]：DNSCrypt は、エンドポイントと DNS サーバー間の DNS クエリを認証および暗号化します。DNScrypt を有効にするには、証明書の検証に DNScrypt の公開キーを設定できます。このキーは、32 バイトの 16 進数値で、B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79 に事前設定されています。これは、Umbrella エニーキャストサーバーの公開キーです。
- [管理キー（Management Key）]：VPN ポリシーのために Umbrella クラウドからデータセンターの詳細を取得するためのキー。
- [管理シークレット（Management Secret）]：VPN のために Umbrella クラウドからデータセンターを取得するために使用されるシークレット。

ステップ 4 [接続のテスト（Test Connection）] をクリックします。Cisco Umbrella Cloud が Management Center から到達可能かどうかをテストします。必要な組織 ID とネットワークデバイスの詳細を指定すると、Cisco Umbrella 接続が作成されます。

ステップ 5 [保存（Save）] をクリックします。

Cisco Umbrella DNS ポリシーを作成する

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（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）] > [Umbrella DNSポリシー（Umbrella 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

ポリシーを設定します。Cisco Umbrella DNS ポリシーとルールの編集 （21 ページ） を参照してください。

Cisco Umbrella DNS ポリシーとルールの編集

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [DNS]**を選択します。

ステップ 2 [DNSポリシー（DNS Policy）] ページで、編集する Cisco Umbrella DNS ポリシーを選択してクリックします。**[編集（Edit）]** （✎）

Cisco Umbrella 保護ポリシーの更新

Cisco Umbrella から最新の Cisco Umbrella 保護ポリシーを取得するには、[Cisco Umbrella保護ポリシーの最終更新日（Umbrella Protection Policy Last Updated）] の横にある [更新（Refresh）] アイコンをクリックします。

Management Center の Cisco Umbrella 接続設定を設定または変更するには、**[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）] > [Cisco Umbrella 接続（Cisco Umbrella Connection）]** に移動します。

ステップ 3 Cisco Umbrella DNS ポリシーエディタで、Cisco Umbrella DNS ルールを選択して **[編集（Edit）]** （✎） をクリックします。

ステップ 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。

- [Cisco Umbrella保護ポリシー（Umbrella Protection Policy）]：デバイスに適用する Cisco Umbrella ポリシーの名前を指定します。

- [バイパスドメイン（Bypass Domain）]：Cisco Umbrella をバイパスして、代わりに設定済みの DNS サーバーに直接移動させるための DNS 要求のローカルドメインの名前を指定します。

  たとえば、すべての内部接続が許可されることを想定して、内部 DNS サーバーで組織のドメイン名のすべての名前を解決できます。

- [Dnscrypt]：DNSCrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。

  DNSCrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNSCrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラスマップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

- [アイドルタイムアウト（Idle Timeout）]：アイドルタイムアウトを設定します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

Cisco Umbrella 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。詳細については、Cisco Umbrella 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る （22 ページ）を参照してください。

Cisco Umbrella 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る

Cisco Umbrella DNS ポリシーは、デバイスに展開する前に、アクセス コントロール ポリシーに関連付ける必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス制御（Access Control）] に移動し、編集するアクセスポリシーを選択します。

ステップ 2 [セキュリティインテリジェンス（Security Intelligence）] を選択します。

ステップ 3 [Cisco Umbrella DNSポリシー（Umbrella DNS Policy）] ドロップダウンリストから、Cisco Umbrella DNS ポリシーを選択します。

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。

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。