QoS

以下のトピックでは、Firewall Threat Defenseデバイスを使ってネットワーク トラフィックを管理するために Quality of Service（QoS）機能を使用する方法について説明します。

QoS の概要

Quality of Service（QoS）は、アクセス制御によって許可または信頼されている（ポリシーの）ネットワーク トラフィックをレート制限します。システムはファストパスされたトラフィックにレート制限は行いません。

QoS は Firewall Threat Defense デバイスのルーテッドインターフェイスでのみサポートされていますが、サイト間 VPN および VTI インターフェイスではサポートされていません。

レート制限された接続のロギング

QoS 用のロギング設定はありません。接続はロギングなしでレート制限することができ、またレート制限されているという理由だけで接続をロギングすることはできません。接続イベントで QoS 情報を表示するには、適切な接続の終了を Firewall Management Center データベースに個別にロギングする必要があります。詳細については、*Cisco Secure Firewall Management Center Administration Guide*の「Other Connections You Can Log」を参照してください。

レート制限された接続の接続イベントには、どの程度のトラフィックがドロップされ、どの QoS の設定がトラフィックを制限したかについての情報が含まれています。この情報はイベント ビューア（ワークフロー）、ダッシュボード、レポートで確認できます。

QoS ポリシーについて

管理対象デバイスに展開する QoS ポリシーによりレート制限が決まります。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

システムは指定した順序で QoS ルールをトラフィックと照合します。システムは、すべての条件がトラフィックに一致する最初のルールに従ってトラフィックをレート制限します。どのルールにも一致しないトラフィックは、レート制限を受けません。

（注） デバイス上の QoS ルールを含むルールの総数は 255 以下である必要があります。このしきい値に達すると、展開警告メッセージが表示されます。正常に展開するには、ルールの数を減らす必要があります。

QoS ルールは、送信元または接続先（ルーティング先）インターフェイスによって制約を設ける必要があります。システムは、これらの個別のインターフェイスでそれぞれ独立したレート制限を行います。複数のインターフェイスにまとめてレート制限を指定することはできません。

QoS ルールでは、その他のネットワーク特性や、アプリケーション、URL、ユーザ ID、およびカスタム セキュリティ グループ タグ（SGT）などのコンテキスト情報によってトラフィックのレート制限を行うこともできます。

ダウンロード トラフィックとアップロード トラフィックは、それぞれ独立してレート制限が可能です。システムは、接続イニシエータを基準としてダウンロードかアップロードかを判別します。

（注） QoS はメインアクセス制御設定に従属するものではありません。QoS は個別に設定します。ただし、同じデバイスに展開されたアクセス コントロール ポリシーおよび QoS ポリシーはアイデンティティ設定を共有します。アクセス制御への他のポリシーの関連付けを参照してください。

QoS の要件と前提条件

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

Access Admin

Network Admin

QoS ポリシーによるレート制限

ポリシー ベースのレート制限を実行するために、管理対象デバイスに QoS ポリシーを設定して展開します。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

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した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に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 **Devices** > **QoS** を選択します。

ステップ 2 [新規ポリシー（New Policy）] をクリックして、新しい QoS ポリシーを作成して、必要に応じてターゲット デバイスを割り当てます。詳細については、QoS ポリシーの作成 （4 ページ）を参照してください。

既存のポリシーを **Copy** () または **Edit** () することもできます。

ステップ 3 QoS ルールを設定します。QoS ルールの設定 （5 ページ）またはQoS ルール条件 （7 ページ）を参照してください。

QoS ポリシーエディタの [ルール（Rules）] には、各ルールが評価順にリストされ、ルール条件とレート制限の設定の概要が表示されます。右クリックのメニューには、ルールの管理オプション（移動、有効化、無効化など）があります。

大規模な展開では、特定のデバイスまたはデバイスのグループに影響するルールのみを表示する、[デバイス基準のフィルタ（Filter by Device）] が役に立ちます。また、ルールの検索とルール内の検索も可能です。システムは、[ルールの検索（Search Rules）] フィールドに入力されたテキストをルールの名前および条件値と照合します。これには、オブジェクトとオブジェクトグループが含まれます。

（注）
ルールを適切に作成して順序付けることは複雑なタスクですが、効果的な展開を構築する上で不可欠なタスクです。慎重に計画していないと、ルールが別のルールをプリエンプション処理したり、追加のライセンスが必要になったり、ルールに無効な設定が含まれる場合があります。アイコンにより、コメント、警告、およびエラーが表されます。問題があれば、[警告の

表示（Show Warnings）] をクリックしてリストを表示します。詳細については、アクセス制御ルールのベストプラクティスを参照してください。

ステップ 4 [ポリシーの割り当て（Policy Assignments）] をクリックして、ポリシーがターゲットにしている管理対象デバイスを特定します。詳細については、QoS ポリシーのターゲット デバイスの設定 （4 ページ）を参照してください。

ポリシーの作成中にデバイス ターゲットを特定した場合は、選択内容を確認します。

ステップ 5 QoS ポリシーを保存します。

ステップ 6 この機能では一部のパケットを通過させる必要があるため、これらのパケットを検査するようにシステムを設定する必要があります。

ステップ 7 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。

QoS ポリシーの作成

ルールのない新規 QoS ポリシーは、レート制限を実行しません。

手順

ステップ 1 **Devices** > **QoS** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 （オプション）ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリックするか、[選択されたデバイス（Selected Devices）] にドラッグ アンド ドロップします。表示されるデバイスを絞り込むには、[検索（Search）] フィールドに検索文字列を入力します。

ポリシーを展開する前に、デバイスを割り当てる必要があります。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- QoS ポリシーを設定および展開します。QoS ポリシーによるレート制限 （3 ページ）を参照してください。

QoS ポリシーのターゲット デバイスの設定

各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

手順

ステップ 1 QoS ポリシー エディタで、[ポリシーの割り当て（Policy Assignments）] をクリックします。

ステップ 2 ターゲット リストを作成します。

- 追加：1 つ以上の [使用可能なデバイス（Available Devices）] を選択して、[ポリシーに追加（Add to Policy）] をクリックするか、[選択したデバイス（Selected Devices）] のリストにドラッグ アンド ドロップします。
- 削除：1 つのデバイスの横にある **Delete** () をクリックするか、複数のデバイスを選択して、右クリックしてから [選択済み項目の削除（Delete Selected）] を選択します。
- 検索：検索フィールドに検索文字列を入力します。検索をクリアするには、**Clear** () をクリックします。

ステップ 3 [OK] をクリックしてポリシーの割り当てを保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

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。

QoS ルールの設定

ルールを作成または編集するときに、一般的なルール プロパティを設定するには、ルール エディタの上部を使用します。ルール条件とコメントを設定するには、ルールエディタの下部を使用します。

手順

ステップ 1 QoS ポリシーエディタの [ルール（Rules）] で、次の操作を実行します。

- ルールの追加：[ルールの追加（Add Rule）] をクリックします。
- ルールの編集：**Edit** () 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 ルール コンポーネントを設定します。

- [有効化（Enabled）]：ルールを有効にするかどうかを指定します。
- [QoS の適用（Apply QoS On）]：レート制限するインターフェイス（[宛先インターフェイス オブジェクトのインターフェイス（Interfaces in Destination Interface Objects）] または [送信元インターフェイス オブジェクトのインターフェイス（Interfaces in Source Interface

Objects）]）を選択します。選択するインターフェイスは、入力されたインターフェイス制約（任意ではなく）と一致する必要があります。

- [インターフェイスごとのトラフィック制限（Traffic Limit Per Interface）]：ダウンロード制限とアップロード制限を Mbits/sec 単位で入力します。[無制限（Unlimited）] のデフォルト値にすると、一致するトラフィックはその方向でレート制限されません。
- [条件（Conditions）]：追加する対応条件をクリックします。[QoS の適用（Apply QoS On）] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント（Comments）]：[コメント（Comments）] をクリックします。コメントを追加するには、[新規コメント（New Comment）] をクリックしてコメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ルール コンポーネントの詳細については、QoS ルール コンポーネント （6 ページ）を参照してください。

ステップ 4 ルールを保存します。

ステップ 5 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。

ルールには 1 から番号が付けられます。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。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 6 [保存（Save）] をクリックして、ポリシーを保存します。

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。

関連トピック

アクセス制御ルールのベストプラクティス

QoS ルール コンポーネント

状態（有効/無効）

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。

インターフェイス（QoS の適用対象）

すべてのトラフィックがレート制限されている QoS のルールは保存できません。QoS のルールごとに、次のいずれかに QoS を適用する必要があります：

- 送信元インターフェイス オブジェクトのインターフェイス：レートは、ルールの送信元インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少

なくとも 1 つの送信元インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。

- 宛先インターフェイス オブジェクト：レートは、ルールの宛先インターフェイスを介するトラフィックに制限されます。このオプションを選択すると、少なくとも 1 つの宛先インターフェイスの制約を追加する必要があります（**どんな**制約であってもよいわけではありません）。

インターフェイスごとのトラフィック制限

QoS ルールでは、[QoS の適用対象（Apply QoS On）] オプションで指定するインターフェイスごとに個別にレートを制限します。インターフェイスのセットに対して集約レート制限を指定することはできません。

トラフィックのレート制限を M ビット/秒とします。[無制限（Unlimited）] のデフォルト値では、一致したトラフィックのレートは制限されません。

ダウンロード トラフィックとアップロード トラフィックは、それぞれ独立してレート制限が可能です。システムは、接続イニシエータを基準としてダウンロードかアップロードかを判別します。

インターフェイスの最大スループットを超える制限を指定すると、システムは一致しているトラフィックのレート制限は行いません。最大スループットはインターフェイスのハードウェア構成による影響を受ける可能性があり、各デバイス（**Devices** > **Device Management**）のプロパティに指定します。

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。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルール エディタ内に独自のタブがあります。詳細については、QoS ルール条件 （7 ページ）を参照してください。

説明

ルールで変更を保存するたびに、コメントを追加することができます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ポリシー エディタでは、システムがそのルールのコメント数を表示します。ルール エディタでは、[コメント（Comments）] タブを使用して、既存のコメントを表示し、新しいコメントを追加します。

QoS ルール条件

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。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。各条件の種類には、ルール エディタ内に独自のタブがあります。以下を使用して、トラフィックをレート制限できます：

詳細については、次の項を参照してください。

関連トピック

インターフェイスルール条件 （8 ページ）
ネットワークルールの条件 （8 ページ）
ユーザー ルール条件 （9 ページ）
アプリケーションルールの条件 （9 ページ）
ポートルールの条件 （11 ページ）
URL ルール条件 （12 ページ）
カスタム SGT ルール条件 （13 ページ）

インターフェイスルール条件

インターフェイス ルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイス オブジェクトを使用してインターフェイス条件を構築できます。インターフェイス オブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィック フローを制御し、分類しやすくします。インターフェイス（Interface）を参照してください。QoS ルールは、ルーテッドインターフェイスのみに適用できます。

ヒント　インターフェイスによってルールを制約するのは、システム パフォーマンスを改善するための最適な方法の 1 つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

ネットワークルールの条件

ネットワークは、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するか、復号します。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。

可能な場合は常に、一致基準の数を最小限にします（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。

（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。

ユーザー ルール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directory レルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの [認証不要（No Authentication Required）] ルールアクションに一致するユーザー。
- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、ID ポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付けを参照）。

アプリケーションルールの条件

システムはIP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーションフィルタの利点

アプリケーションフィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーションフィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーショントラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーショントラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *1*: アプリケーションの特性

特性	説明	例
タイプ	アプリケーション プロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

ポートルールの条件

ポート条件を使用することで、トラフィックの送信元および宛先のポートに応じてそのトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（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。

ポートベースのルールのベストプラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（Firewall Threat Defense など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

ポート、プロトコル、および ICMP コード ルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（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。

ポートベースのルールのベスト プラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーション フィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーション フィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して**すべての**トラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。
- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

URL ルール条件

URL 条件を使用してネットワークのユーザーがアクセスできる Web サイトを制御します。

詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについてを参照してください。

カスタム SGT ルール条件

ID ソースとして ISE/ISE-PIC を設定しない場合、ISE によって指定**されていない**セキュリティ グループ タグ（SGT）使用してトラフィックを制御できます。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。

カスタム SGT ルールの条件では、システムが ISE サーバとの接続によって取得した ISE SGT ではなく、手動で作成された SGT オブジェクトを使ってトラフィックをフィルタ処理します。この手動で作成された SGT オブジェクトは、制御するトラフィックの SGT 属性に対応します。カスタム SGT を使用したトラフィック制御は、ユーザ制御とは見なされません。

ISE SGT とカスタム SGT ルール条件との比較

ルールの中には、割り当てられた SGT に基づいてトラフィックを制御するために使用できるものがあります。ルールのタイプ、およびアイデンティティ ソースの設定によって、ISE 割り当ての SGT またはカスタム SGT のいずれかを使用して、トラフィックを割り当て済み SGT 属性と照合することができます。

（注） ISE SGT を使用してトラフィックを照合する場合、パケットに SGT 属性が割り当てられていないとしても、パケットの送信元 IP アドレスが ISE 内で既知であれば、そのパケットは ISE SGT ルールと照合されます。

条件タイプ	要件	ルール エディタにリストされている SGT
ISE SGT	ISE アイデンティティ ソース	ISEサーバをクエリして取得され、メタデータが自動的に更新される SGT
カスタム SGT	ISE/ISE-PIC アイデンティティ ソースなし	ユーザーが作成するスタティック SGT オブジェクト

カスタムセキュリティグループタグ（SGT）からISEセキュリティグループタグ（SGT）への自動遷移

カスタム SGT に一致するルールを作成し、ISE/ISE-PIC を ID ソースに設定すると、システムは次の動作をします。

- オブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを無効にします。システムは既存の SGT オブジェクトをそのまま保持しますが、それらの変更や、新しいオブジェクトの追加はできません。
- カスタム SGT 条件の既存のルールを保持します。ただし、これらのルールはトラフィックの照合を行いません。また、既存のルールにカスタム SGT 基準を追加することや、カスタム SGT 条件を含む新しいルールを作成することはできません。

ISEを設定する場合は、カスタムSGT条件を含む既存のルールは削除するか、無効にすることを推奨します。SGT属性を持つトラフィックを照合するには、代わりにISE属性条件を使用します。

QoS の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
廃止：FlexConfig での priority-queue。	7.2.5	7.2.5	FlexConfig は、Threat Defense で priority-queue を設定するために使用されていました。このコマンドは削除されました。
レピュテーションが不明な URL の処理を指定する機能。	6.7.0	いずれか	詳細については、URL フィルタリングの履歴を参照してください。 新しい/変更された画面：QoS ルールエディタ
レート制限の増大。	6.2.1	いずれか	最大レート制限が 1,000 Mbps から 100,000 Mbps に増やされました。 新しい/変更された画面：QoS ルールエディタ
カスタム SGT および元のクライアントネットワーク フィルタリング。	6.2.1	いずれか	カスタム セキュリティ グループ タグ（SGT）および元のクライアントネットワーク情報（XFF、True-Client-IP、またはカスタム定義の HTTP ヘッダー）を使用した、トラフィックのレート制限。 新しい/変更された画面：QoS ルールエディタ
QoS（レート制限）の導入。	6.1.0	いずれか	FTDは、アクセス制御によって許可または信頼されている（ポリシーの）ネットワークトラフィックをレート制限します。 新しい/変更された画面：**[デバイス（Devices）] > [QoS]**

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。