Firepower Threat Defense 用の Quality of Service（QoS）

以下のトピックでは、Firepower 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、Firepower Threat Defense デバイスのルーテッド インターフェイスのみでサポートされています。

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 Firepower 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。ログ可能なその他の接続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（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。

QoS ポリシーでは、最大 32 の QoS ルールがネットワーク トラフィックを処理します。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。

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。

トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続イニシエータに基づいてダウンロード方向とアップロード方向を決定します。

（注） QoS はマスター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 ポリシーとマルチテナンシー

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。

先祖ドメインの管理者は、異なる子孫ドメインのデバイスに、同じ QoS ポリシーを展開できます。子孫ドメインの管理者は、この先祖ドメインから展開された読み取り専用 QoS ポリシーを使用するか、またはローカル ポリシーに置き換えることができます。

QoS ポリシーによるレートの制限

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）
任意（Any）	該当なし	FTD	任意（Any）	Admin/Access Admin/Network Admin

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ターゲットにすることができます。各デバイスに同時に展開できる 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。

また、既存のポリシーをコピー（  ）または編集（  ）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 （6 ページ）またはルール管理：共通の特性を参照してください。

QoS ポリシー エディタの [ルール（Rules）] タブには、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、ルールのパフォーマンスに関するガイドライン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 （5 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 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

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）
任意（Any）	該当なし	FTD	任意（Any）	Admin Access Admin Network Admin

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の制限 （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

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）
任意（Any）	該当なし	FTD	任意（Any）	Admin Access Admin Network Admin

各 QoS ポリシーは複数のデバイスをターゲットにすることができます。各デバイスに同時に展開できる 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削除アイコン（）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、クリア（）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

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）
任意（Any）	該当なし	FTD	任意（Any）	Admin/Access Admin/Network Admin

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、下部のタブを使用します。

手順

ステップ 1 QoS ポリシー エディタの [ルール（Rules）] タブで、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：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 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）]：追加する条件に対応するタブをクリックします。[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）] タブをクリックします。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 （7 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

ルールのパフォーマンスに関するガイドライン

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。

トラフィックのアップロードやダウンロードのレート制限を個別に行うことが可能です。システムは、接続イニシエータに基づいてダウンロード方向とアップロード方向を決定します。

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（Conditions）

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。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：

- インターフェイス条件 （ルート設定済みの場合のみ、必須）
- ネットワーク条件
- ポートおよび ICMP コードの条件
- アプリケーション条件（アプリケーション制御）
- URL フィルタリング
- ユーザ条件、レルム条件、および ISE 属性条件（ユーザ制御）
- カスタム SGT 条件

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 の履歴

機能	バージョン（Version）	詳細
レート制限の増大	6.2.1	最大レート制限が 1,000 Mbps から 100,000 Mbps に増やされました。 変更された画面：QoS ルール エディタ サポートされているプラットフォーム：Firepower Threat Defense

機能	バージョン（Version）	詳細
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	QoS では、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）を使用して、トラフィックのレート制限を行えるようになりました。 変更された画面：QoS ルール エディタ サポートされているプラットフォーム：Firepower Threat Defense
QoS（レート制限）	6.1	導入された機能。 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。 新しい画面：**[デバイス（Devices）] > [QoS]** サポートされているプラットフォーム：Firepower Threat Defense