



QoS の設定

QoS とは、選択されたネットワーク トラフィックにさまざまな技術を通してよりよいサービスを提供することにより、基盤となる技術の限られた帯域幅で全体として最適なサービスを実現するネットワークの機能です。

セキュリティ アプライアンスでの QoS の第 1 の目的は、個々のフローと VPN トンネル フローの両方について選択したネットワークにレート制限を提供し、限られた帯域幅をすべてのトラフィックが公正に共有できるようにすることです。フローは複数の方法で定義できます。セキュリティ アプライアンスでは、QoS は送信元 IP アドレスと宛先 IP アドレス、送信元ポート番号と宛先ポート番号、および IP ヘッダーの TOS バイトの組み合わせに適用できます。

ここでは、次の項目について説明します。

- [QoS サービス ポリシーの設定 \(P. 28-2\)](#)
- [Priority Queue \(P. 28-4\)](#)

QoS サービス ポリシーの設定

QoS サービス ポリシーは、標準のサービス ポリシーと同じ方法で作成します。次の手順は、標準のサービス ポリシー作成プロセスの概要です。そのサービス ポリシーの QoS 機能の設定部分に重点を置いて説明しています。サービス ポリシー ルール作成の詳細については、[P.23-5 の「通過トラフィックのサービス ポリシー ルールの追加」](#)を参照してください。

QoS サービス ポリシーを設定するには、次の手順を実行します。

ステップ 1 **Configuration > Firewall > Service Policy Rules** ペインを開きます。

ステップ 2 **Add** をクリックして新しいサービス ポリシー ルールを作成します。

Service Policy Wizard が開きます。

ステップ 3 サービス ポリシー ルールのスコープを定義します。サービス ポリシー ルールは、グローバルに(すべてのインターフェイスに)適用することも、特定のインターフェイスに適用することもできます。**Next** をクリックします。

ステップ 4 サービス ポリシーで照合するトラフィックを定義します。選択した照合基準に応じて、いくつかのウィザード画面を使用して設定する必要があります。照合基準の設定の詳細については、[P.23-5 の「通過トラフィックのサービス ポリシー ルールの追加」](#)を参照してください。**Next** をクリックします。

Rules Actions 画面が表示されます。

ステップ 5 **QoS** タブをクリックします。

ステップ 6 QoS を設定するには、次の手順を実行します。

- 指定したトラフィックをプライオリティの高いトラフィックとして定義するには、**Enable priority for this flow** をクリックします。これにより、トラフィックが高プライオリティとして定義され、プライオリティキューを設定できるようになります。このオプションを選択するとトラフィック ポリシングはイネーブルにできません。
- トラフィックのレート制限を設定するには、**Enable policing** をクリックします。これにより、入力または出力（または両方）のトラフィック レートの制限、バースト レートの定義、および適合トラフィックと非適合トラフィックに対して実行するアクションの指定を行うことができます。これらの設定の詳細については、[P.28-3 の「QoS タブのフィールド情報」](#)を参照してください。

ステップ 7 **Finish** をクリックします。サービス ポリシー ルールがルール テーブルに追加されます。**Apply** をクリックしてコンフィギュレーションをデバイスに送信します。

ステップ 8 トラフィックのプライオリティをイネーブルにした場合、特定のインターフェイスのプライオリティキューを設定する必要があります。プライオリティキューの設定の詳細については、[P.28-4 の「Priority Queue」](#)を参照してください。

QoS タブのフィールド情報

QoS タブでは、厳密なスケジュールプライオリティとレート制限トラフィックを適用できます。

制約事項

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

フィールド

- **Enable Priority for this flow** : このフローでの厳密なスケジュールプライオリティをイネーブルまたはディセーブルにします。プライオリティは、プライオリティキューが設定されるまで有効になりません。プライオリティキューを設定するには、P.28-4 の「Priority Queue」を参照してください。
- **Enable policing** : 入力および出力のトラフィック ポリシングをイネーブルにするには、このチェックボックスをオンにします。続いて、指定したタイプのトラフィック ポリシングをイネーブルにするには、**Input policing** または **Output policing**（または両方の）チェックボックスをオンにします。トラフィック ポリシングのタイプごとに、次のフィールドを設定します。
 - **Committed Rate** : このトラフィック フローのレート制限。これは、8000 ~ 2000000000 の範囲の値で、許容最大速度（bps）を指定します。
 - **Conform Action** : レートが適合バースト値未満の場合に実行するアクション。値は、transmit または drop です。
 - **Exceed Action** : レートが適合レート値と適合バースト値の間になっている場合に、このアクションを実行します。値は、transmit または drop です。
 - **Burst Rate** : 1000 ~ 512000000 の範囲の値で、適合レート値までトラフィックを抑制するまでに、持続したバーストにおいて許可される瞬間的なバイト数を指定します。



(注) Enable Policing チェックボックスをオンにすると、最大速度とバースト レートが適用され、適合レート値になるよう強制されます。**適合アクション**または**超過アクション**の指定があっても、それらは適用されません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	—	•	—	—

Priority Queue

QoS サービス ポリシー ルールを定義し、その中でトラフィックを高プライオリティに設定した場合、1 つ以上のインターフェイスでプライオリティキューをイネーブルにし、それらのインターフェイスを通過するトラフィックに対してサービス ルールがイネーブルになるようにする必要があります。プライオリティ キューイングは、デフォルトでディセーブルになっています。**Configuration > Device Management > Advanced > Priority Queue** に移動し、プライオリティキューを設定します。

Priority Queue ペインに Priority Queue テーブルが表示されます。Priority Queue テーブルには、プライオリティキューが設定されるインターフェイスごとに次の情報が表示されます。

- **Interface** : キューが設定されるインターフェイスです。
- **Queue Limit** : 通常キューまたはプライオリティキューに入れることができるパケットの最大数です。この最大数を超えると接続をドロップします。どちらのキューも上限値は同じです。プライオリティキュー内のパケットは、通常のプライオリティキューのパケットが送信される前に完全に排出されます。
- **Transmission Ring Limit** : プライオリティキューの深さを指定します。プライオリティ キューイングがイネーブルになっていないと、このカラムに「Ring Disabled」というメッセージが表示されます。

プライオリティキューのコンフィギュレーションを追加または変更するには、次の手順を実行します。

- 新しいプライオリティキューを追加するには、**Add** をクリックします。Add Priority Queue ダイアログボックスが表示されます。
- 既存のプライオリティキューを編集するには、テーブルでキューのエントリをクリックし、**Edit** をクリックします。または、テーブルでキューのエントリをダブルクリックします。Edit Priority Queue ダイアログボックスが表示されます。

フィールド

Add/Edit Priority Queue ダイアログボックスには次のフィールドがあります。

- **Interface** : プライオリティキューをイネーブルにするインターフェイスを選択します。インターフェイスごとに設定できるプライオリティキューは 1 つのみです。このフィールドには、プライオリティキューが設定されていないインターフェイスがすべて表示されます。
- **Queue Limit** : 通常キューまたはプライオリティキューに入れることができるパケットの最大数を指定します。この最大数を超えると接続をドロップします。最小パケット数は 0 です。最大数は実行時に使用可能なメモリに基づいてダイナミックに決まります。理論上の最大パケット数は 2147483647 です。



(注) どちらのキューも上限値は同じです。プライオリティキュー内のパケットは、通常のプライオリティキューのパケットが送信される前に完全に排出されます。

- **Transmission Ring Limit** : Ethernet 伝送ドライバに送ることができる低遅延または通常プライオリティのパケットの最大数を指定します。この最大数を超えると、Ethernet 伝送ドライバがインターフェイスのキューにパケットを押し戻し、輻輳が解消されるまでパケットをキューにバッファします。最小値は 3 です。範囲の上限値は実行時にダイナミックに決まります。主な決定要素は、キューのサポートに必要なメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリ容量を超えないようにする必要があります。理論上の最大パケット数は 2147483647 です (つまり、全二重の回線速度に対応します)。プライオリティ キューイングがイネーブルになっていないと、このカラムに「Ring Disabled」というメッセージが表示されます。

伝送リング制限値とは、ドライバがインターフェイスの前に配置されたキューにパケットを押し戻し、輻輳が解消されるまでパケットをバッファに入れる前に、ドライバに送ることを許可するいずれかのタイプのパケットの数のことです。通常は、`queue-limit` パラメータと伝送リング制限パラメータを調整し、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これがテールドロップです。キューがいっぱいになることを避けるため、`queue-limit` パラメータを調整してキューのバッファサイズを大きくすることができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

