CHAPTER 28

QoS の設定

QoS は、基盤となるテクノロジーの限られた帯域幅で全体的に最良のサービスを実現するさまざまなテクノロジーによって、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの機能を指します。

セキュリティ アプライアンスでの QoS の主要な目的は、個別のフローおよび VPN トンネル フローの両方で、選択したネットワーク トラフィックのレートを制限し、限られた帯域幅の中ですべてのトラフィックが適切な割り当て分を得ることができるようにすることです。フローはさまざまな方法で定義できます。セキュリティ アプライアンスでは、送信元 IP アドレスと宛先 IP アドレスの組み合わせ、送信元ポート番号と宛先ポート番号の組み合わせ、および IP ヘッダーの TOS バイトに QoS を適用できます。

ここでは、次の内容について説明します。

QoS サービス ポリシーの設定

QoS サービス ポリシーは、通常のサービス ポリシーと同様の方法で作成されます。この手順では、通常のサービス ポリシーの作成プロセスの概要を示し、そのサービス ポリシーの QoS 機能の設定に重点を置いています。サービス ポリシー ルールの作成の詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）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 ルールの範囲を定義します。サービス ポリシー ルールは、グローバル（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 ポリシーに一致するトラフィックを定義します。選択した一致基準によっては、複数のウィザード画面が表示され、順に実行する必要がある場合があります。一致基準の設定の詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）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、次のいずれかの操作を実行します。

- 特定の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、そのプライオリティ 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、「[QoS] タブのフィールド情報」（P.28-2）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、「プライオリティ キュー」（P.28-3）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

確立済みの VPN クライアント/LAN-to-LAN または非トンネル トラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリア（つまりドロップ）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、「プライオリティ キュー」（P.28-3）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。次に、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（ビット/秒）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最大瞬間バイト数を指定します。

（注）　[Enable Policing] チェックボックスは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的に合わせるだけです。**conform-action** または **exceed-action** の指定は、存在する場合でも適用されません。

モード

次の表は、この機能を使用できるモードを示したものです。

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

プライオリティ キュー

トラフィックを高プライオリティとして定義する QoS サービス ポリシー ルールを定義した場合は、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です。プライオリティ キューを設定するには、[Configuration] > [Device Management] > [Advanced] > [Priority Queue] に移動します。

[Priority Queue] ペインは、プライオリティ キュー テーブルを表示します。[Priority Queue] テーブルは、プライオリティ キューが設定されているインターフェイスごとに次の情報を表示します。

- [Interface] : キューが設定されたインターフェイス。
- [Queue Limit] : 接続がドロップされるまでの、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。両方のキューに同じ制限があります。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 キュー内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でない場合、このカラムはメッセージ「Ring Disabled」を表示します。

プライオリティ キュー コンフィギュレーションを追加または変更するには、次のいずれかを実行します。

- 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 1 つのプライオリティ キューのみを設定できます。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]：接続がドロップされるまでの、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。最小値は 0 パケットで、最大は、利用可能なメモリに基づいて実行時に動的に決まります。理論的な最大パケット数は、2147483647 です。

（注） 両方のキューに同じ制限があります。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 キュー内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]：イーサネット送信ドライバが受け入れる低遅延パケットまたは通常プライオリティ パケットの最大数を設定します。この制限に達すると、ドライバはパケットをインターフェイスのキューに差し戻し、輻輳が解消されるまでパケットをバッファに格納できるようにします。最小値は 3 です。値の範囲の上限は、実行時にダイナミックに決定されます。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論上の最大パケット数は 2147483647（つまり、全二重回線速度まで）です。プライオリティ キューイングがイネーブルでない場合、このカラムはメッセージ「Ring Disabled」を表示します。

  伝送リング制限は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。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には、queue-limit パラメータを調整して、キューのバッファ サイズを大きくします。

モード

次の表は、この機能を使用できるモードを示したものです。

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