トラフィック管理の設定

この章では、次の設定タスクについて説明します。

- ロード バランシングの設定
- VPN トラフィック用の Quality of Service の設定

ロード バランシングの設定

リモート クライアント コンフィギュレーションで、同じネットワーク上に接続された 2 つ以上の ASA を使用してリモート セッションを処理している場合、セッション ロードを共有するようにこれらのデバイスを設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングを使用すると、ロード量が最小のデバイスにセッション トラフィックが誘導されるため、ロードはすべてのデバイスに分散されます。このロード バランシングにより、システム リソースを効率的に使用し、高いアベイラビリティを実現できます。

ロード バランシングを実装するには、同じサブネット上の 2 つ以上のデバイスを論理的にグループ化して*仮想クラスタ*を形成します。

仮想クラスタ内のすべてのデバイスに、セッション ロードが課せられます。仮想クラスタ内の 1 つの ASA である*仮想クラスタ マスター*は、接続を受け入れ、*バックアップ デバイス*と呼ばれる他のデバイスに着信コールを誘導することができます。仮想クラスタ マスターは、クラスタ内のすべてのデバイスを監視し、各デバイスの通信量を追跡し、それに応じてセッション ロードを分散させます。仮想クラスタ マスターは、1 つの物理デバイスに関連付けられているものではなく、デバイス間を移動してその役割を果たします。たとえば、現在の仮想クラスタ マスターに障害が発生すると、クラスタ内のバックアップ デバイスの 1 つがその役割を引き継ぎ、ただちに新しい仮想クラスタ マスターになります。

外部のクライアントには、仮想クラスタは単一の*仮想クラスタ IP アドレス*として見えます。この IP アドレスは特定の物理デバイスに関連付けられていません。現在の仮想クラスタ マスターに属しています。そのため「仮想」です。接続の確立を試行している VPN クライアントは、最初にこの仮想クラスタ IP アドレスに接続します。次に仮想クラスタ マスターは、クラスタ内で使用可能で、ロード量が最小のパブリック IP アドレスを、クライアントに返送します。2 回目のトランザクション（ユーザには透過）では、クライアントはそのデバイスに直接接続します。このような方法で、仮想クラスタ マスターは、リソース間で均等かつ効率的にトラフィックを誘導します。

クラスタ内のあるデバイスに障害が発生した場合、終了されたセッションは、ただちに仮想クラスタ IP アドレスに再接続できます。次に、仮想クラスタ マスターは、それらの接続をクラスタ内のアクティブ デバイスに誘導します。仮想クラスタ マスター自体に障害が発生した場合、クラスタ内のバックアップ デバイスの 1 つが、ただちに、また自動的に、新しい仮想セッション マスターとして役割を引き継ぎます。クラスタ内の複数のデバイスに障害が発生しても、クラスタ内のいずれか 1 つのデバイスがアップ状態で使用可能であれば、ユーザはクラスタへの接続を継続できます。

（注） WebVPN でロード バランシングが正しく機能するには、クラスタ内のすべてのデバイスが WebVPN をサポートしている必要があります。

前提条件

ロード バランシングは、デフォルトではディセーブルです。明示的に設定してイネーブルにする必要があります。

ロード バランシングを設定できるようにするには、まずパブリック インターフェイスおよびプライベート インターフェイスを設定し、仮想クラスタ IP アドレス用のインターフェイスを定義する必要があります。

クラスタ内のすべてのデバイスは、次の値について、クラスタ固有の同じ値を共有する必要があります。

- 仮想クラスタの IP アドレス
- 暗号化設定（オプション）
- 暗号鍵（暗号化がイネーブルでない場合はオプション）
- ポート ID（デフォルト UDP は 9023）

コンフィギュレーション手順の概要

最小の VPN ロード バランシング スキームを設定するには、次の手順を実行します。

1. 仮想クラスタ IP アドレスを定義します。この IP アドレスは、VPN ロード バランシング クラスタ内のすべてのデバイスで共有されます。アドレスは、デバイスで共有されるパブリック サブネット アドレスの範囲内にする必要があります。
2. ステートフル フェールオーバーを設定する場合、暗号化をイネーブルにし、クラスタ内のすべてのデバイスで共有する暗号鍵を定義します。仮想クラスタ内のデバイスは、IPSec を使用して LAN 間トンネル経由で通信します。暗号化をイネーブルにすると、デバイス間で通信されるすべてのロード バランシング情報の暗号化が保証されます。
3. オプションで、クラスタ内のデバイスのデフォルトの優先順位を変更します。範囲は 1 ～ 10 で、10 が最上位です。優先順位は、起動時または既存のマスターに障害が発生したときに、当該デバイスが仮想クラスタ マスターになる可能性を示すものです。設定する優先順位が高いほど、そのデバイスが仮想クラスタ マスターになる可能性は高くなります。
4. クラスタに含まれる各 ASA で、ロード バランシングをイネーブルにします。

この項の例では、次の値を設定します。

- クラスタ IP アドレスは 209.165.202.224。
- クラスタ暗号鍵は、12345678。
- このクラスタでは暗号化がイネーブル。
- この例の ASA の優先順位は 10。

この項の例では、次の CLI コマンドを使用してロード バランシングを設定します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 10
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

CLI コマンドを使用した手順

show running-config vpn load-balancing コマンドを入力すると、特定のグループ ポリシーの実行コンフィギュレーションを表示できます。

CLI を使用してロード バランシングを設定する手順は、次のとおりです。

ステップ 1　**vpn load-balancing** コマンドを実行すると、config-load-balancing モードに移行します。このモードで、クラスタのパラメータを設定します。このモードで **cluster** コマンドを入力して、仮想クラスタ IP アドレスを設定する手順は次のとおりです。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

ステップ 2　このコンフィギュレーションで暗号化を使用するには、**cluster** コマンドを使用し、暗号鍵を定義してから暗号化をイネーブルにします。このステップはオプションです。暗号化をイネーブルにする前に、暗号鍵を設定する必要があります。

```
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster encryption
```

ステップ 3　（オプション）ASA のデフォルトの優先順位を変更するには、**priority** コマンドを次のように使用します。

```
hostname(config-load-balancing)# priority 10
```

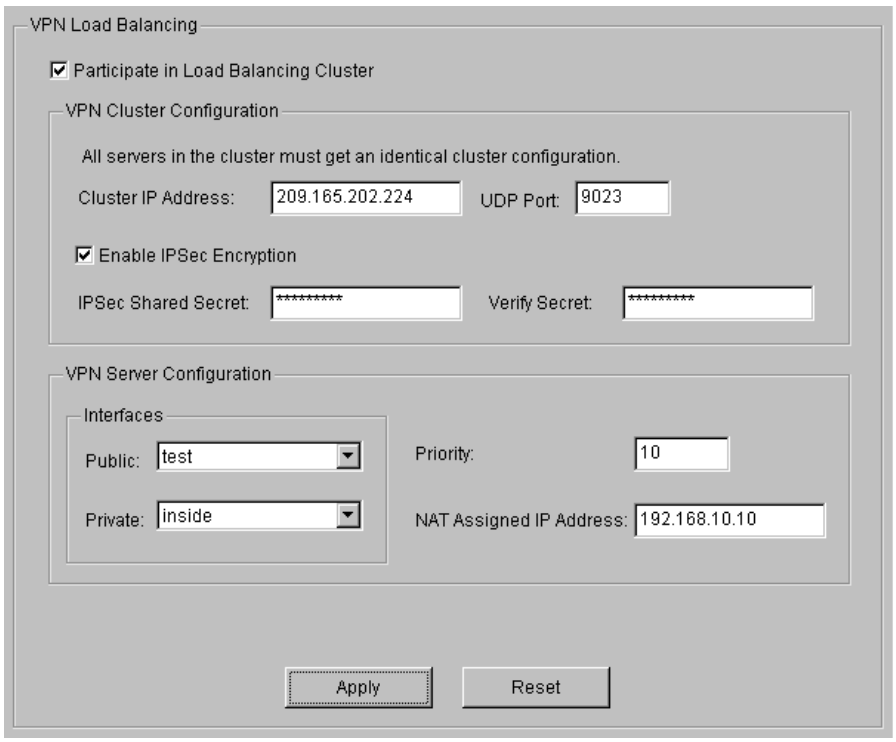
ステップ 4　この ASA でロード バランシングをイネーブルにするには、**participate** コマンドを次のように使用します。

```
hostname(config-load-balancing)# participate
```

ASDM を使用した手順

次の手順は、ASDM を使用してロード バランシングを設定する方法を示しています。この例のパラメータの多くにはデフォルト値があるので、注意してください。

図 6-1　ASDM でのロード バランシングの設定



ステップ 1　VPN ロード バランシングをイネーブルにするには、**Configuration > Features > VPN > Load Balancing** に移動して、**Participate in Load Balancing Cluster** をクリックします。

ステップ 2　**VPN Cluster Configuration** グループ ボックスで、クラスタに参加するすべての ASA 用のパラメータを次のように設定します。

a. **Cluster IP Address** テキスト ボックスにクラスタの IP アドレスを入力します。

b. **Enable IPSec Encryption** オプションをクリックします。

c. **IPSec Shared Secret** テキスト ボックスに暗号鍵を入力し、**Verify Secret** テキスト ボックスにもう一度入力します。

ステップ 3　**VPN Server Configuration** グループ ボックスで次のようにオプションを設定します。

a. **Public** リストで、着信 VPN 接続を受け入れるインターフェイスを選択します。

b. **Private** リストで、プライベート インターフェイスであるインターフェイスを 1 つ選択します。

c. （オプション）**Priority** テキスト ボックスで、ASA でクラスタに対して設定されている優先順位を変更します。

d. このデバイスが、NAT を使用するファイアウォールの背後にある場合は、**NAT Assigned IP Address** に IP アドレスを入力します。この例では、NAT で割り当てられている IP アドレスは 192.168.10.10 です。デバイスが NAT を使用していない場合、または ASA が、NAT を使用するファイアウォールの背後にない場合は、0.0.0.0 と入力します。

VPN トラフィック用の Quality of Service の設定

VPN 3000 コンセントレータには、トラフィック ポリシー管理の一部として帯域幅管理が実装されています。ASA のセキュリティ ポリシー コンフィギュレーションのコンポーネントである Quality of Service（QoS）は、その実装に取って代わるものです。ASA での QoS の実装は、IOS でのその機能の実装に基づいています。

QoS は、ミッション クリティカルなデータと通常のデータの両方にネットワーク リソースを割り振るためのトラフィック管理方針で、この割り振りは、ネットワーク トラフィックのタイプとそのトラフィックに割り当てられた優先順位に基づいて実行されます。簡潔に言うと、QoS は妨害のない優先トラフィックを保証し、レート制限（ポリシング）トラフィック機能を提供します。

QoS は、個々のユーザ トンネルおよびサイトツーサイト トンネルに対して、最大のレート制御またはポリシングを提供します（LAN 間接続では、1 つのトンネル内の個々のユーザ トラフィックは考慮されません）。このリリースでは、最小帯域幅保証（帯域幅予約）は提供されていません。

QoS は大量のリソースを消費し、ASA のパフォーマンスを低下させる可能性があるので、QoS はデフォルトではディセーブルになっています。

次の項では、QoS を使用して、トンネル グループだけの優先トラフィックを設定する方法を簡潔に示します。

（注） QoS の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

コンフィギュレーション手順の概要

ASDM を使用して QoS を設定する手順は、次のとおりです。

1. サービス ポリシーを設定します。

   インターフェイスごとに、またはグローバル レベルで設定できるサービス ポリシーは 1 つだけです。
2. サービス ポリシー規則のトラフィック分類基準を設定します。
3. サービス ポリシー規則で分類されたトラフィックに対するアクションを設定します。

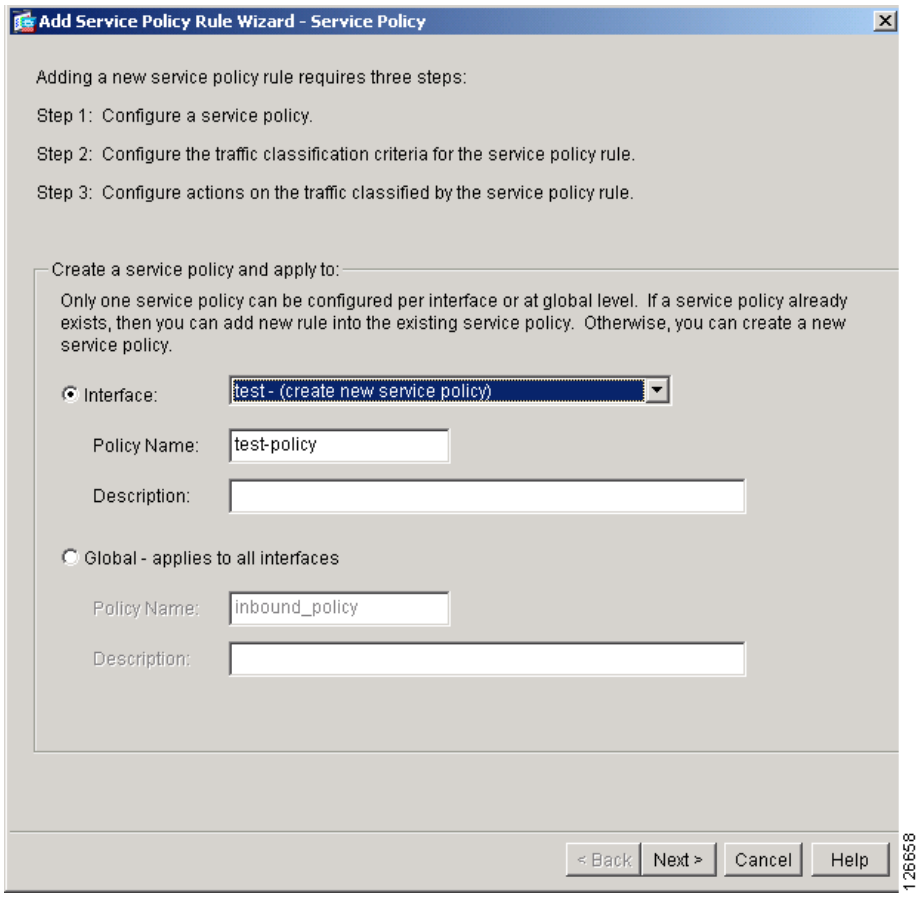
ASDM を使用した手順

ASDM には、QoS の設定手順を紹介するウィザードがあります。この項では、このウィザードを使用してトンネル グループの QoS を設定する方法を示します。ASDM で **Help** ボタンをクリックすると、詳細な情報を参照できます。

ステップ 1　**Configuration > Features > Security policy** パネルで、**Service Policy Rules** をクリックします。

ステップ 2　**Add** をクリックします。ASDM に **Add Service Policy Rule Wizard - Service Policy** ダイアログボックスが表示されます。このダイアログボックスを使用して、サービス ポリシーを作成または編集します。

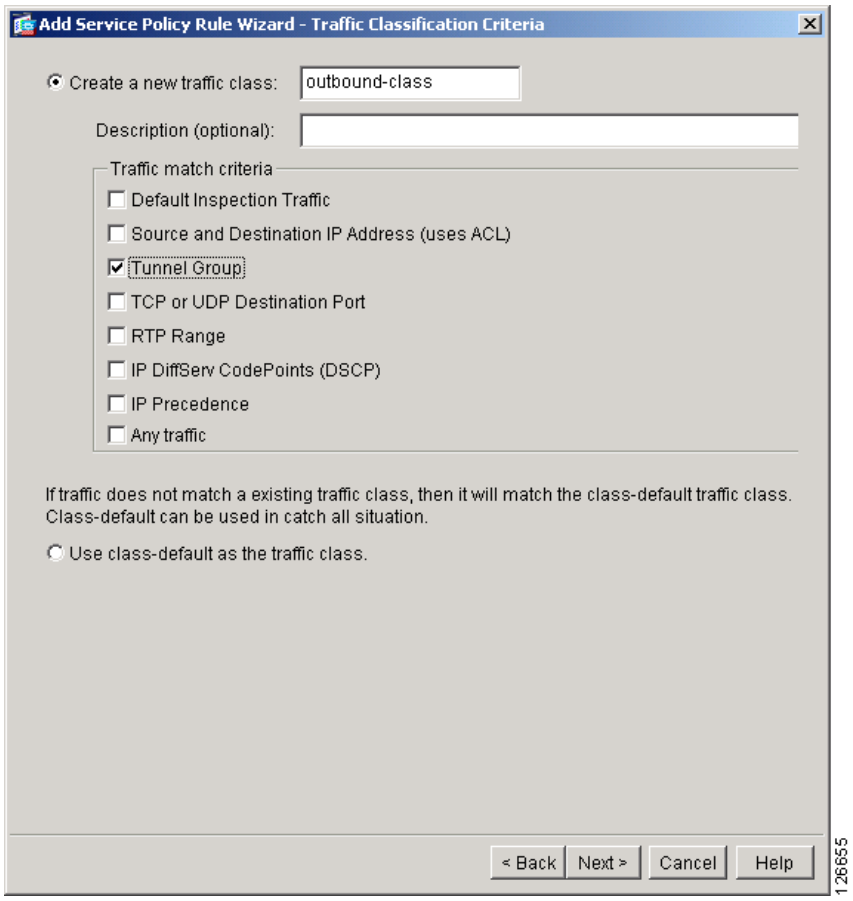
図 6-2　Add Service Policy Rule Wizard - Service Policy ウィザード



ステップ 3　この例では、新しいサービス ポリシーを作成し、そのポリシーをテスト インターフェイスに適用します。開始するには、**Interface** オプションをクリックし、次に **Interface** リストから **test - (create new service policy)** という名前を選択します（インターフェイス名に (create new service policy) というテキストが付加されます）。

ステップ 4　**Policy Name** テキスト ボックスにポリシーの名前を入力します。ASDM では、インターフェイス名に「policy」という言葉を付加したデフォルト名が提供されます。この例では、名前を outbound-policy に変更します。**Next** をクリックします。ASDM に **Add Service Policy Rule Wizard - Traffic Classification Criteria** ダイアログボックスが表示されます。

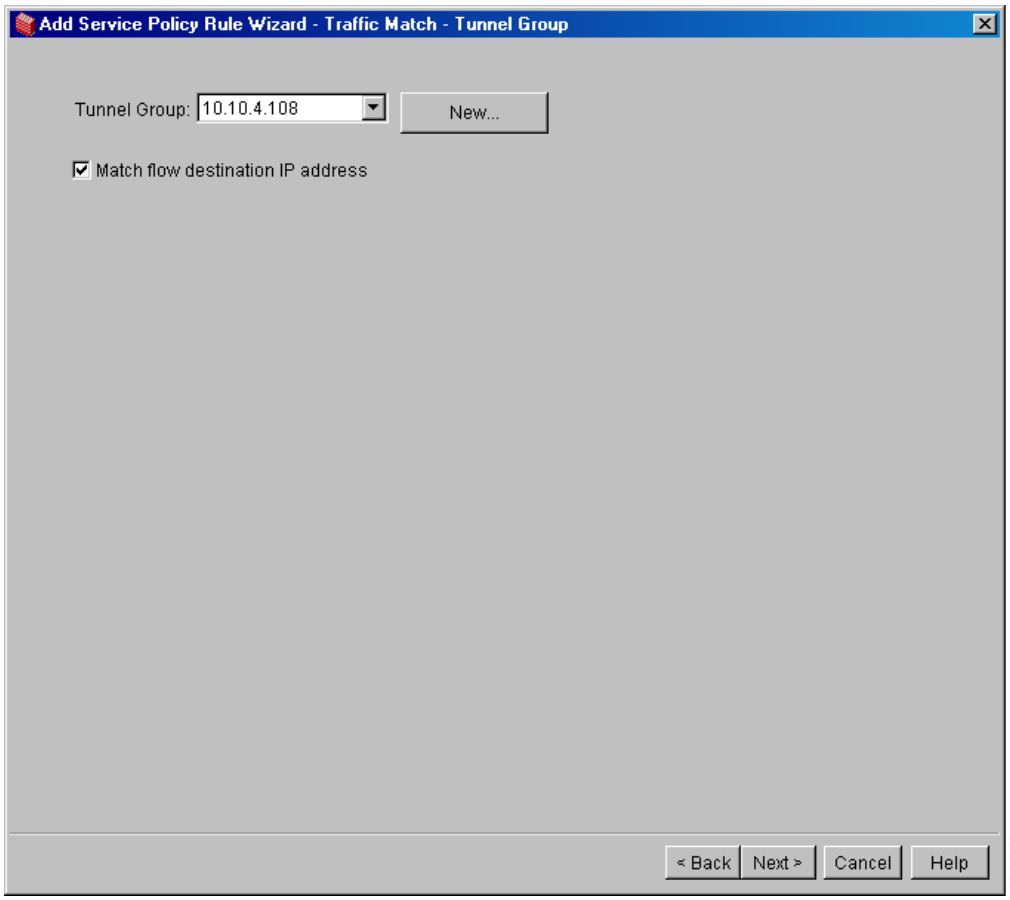
図 6-3　Add Service Policy Rule Wizard - Traffic Classification Criteria



ステップ 5　**Create a new traffic class** オプションをクリックします。ASDM によりインターフェイス名と「class」という言葉が結合されて、テキスト ボックスにデフォルトのポリシー名が作成されます。この例では、名前を outbound-class に変更します。

ステップ 6　**Traffic match criteria** グループ ボックスには、ASA で提供されている一致基準のサブセットが表示されます。この例では、**Tunnel Group** オプションをクリックして、**Next** をクリックします。ASDM に **Add Service Policy Rule Wizard-Traffic Match - Tunnel Group** ダイアログボックスが表示されます。

図 6-4　Add Service Policy Rule Wizard-Traffic Match - Tunnel Group

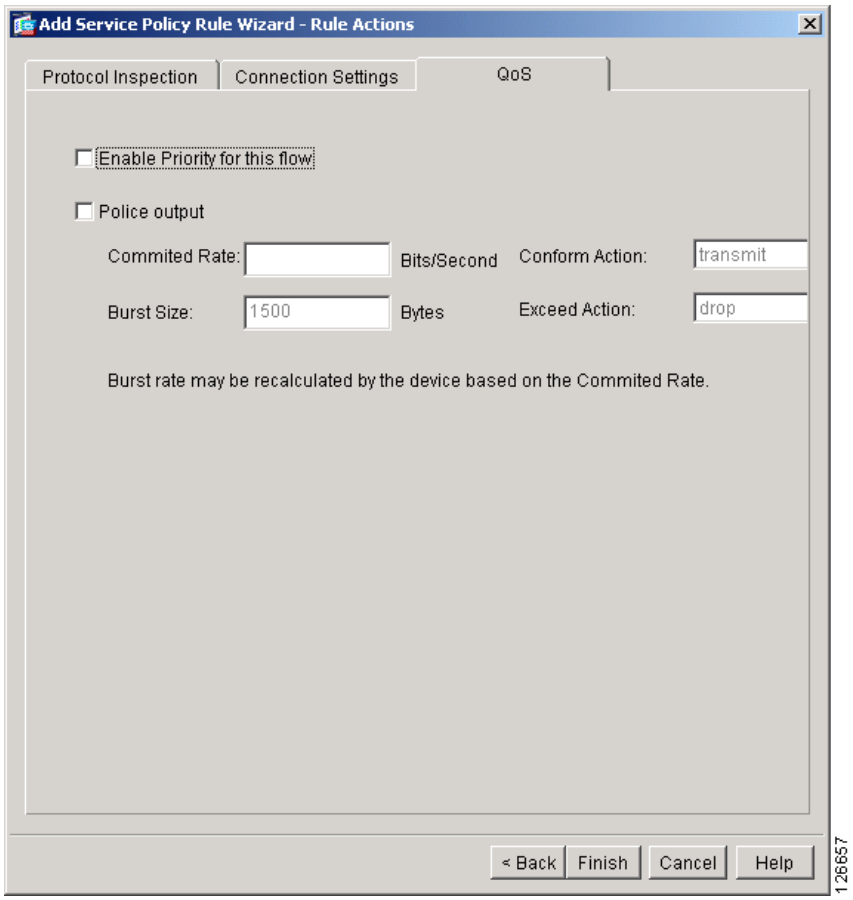


ステップ 7　システムにすでに存在するトンネル グループの IP アドレスを選択するか、**New** をクリックして新しいトンネル グループを設定します。この例では、**Tunnel Group** リストから **10.10.4.108** を選択し、**Match flow destination IP address** をクリックします。このオプションをイネーブルにすると、次のダイアログボックスで選択するトラフィック アクションが、このトンネル グループに適用されます。**Next** をクリックします。

ASDM に **Add Service Policy Rule Wizard - Rule Actions** ダイアログボックスが表示されます。

ステップ 8　**QoS** タブをクリックします。

図 6-5　QoS オプションの設定



QoS タブでは、次の規則アクションの 1 つを選択できます。

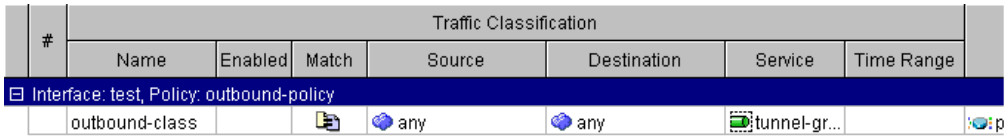
- **Enable Priority for this flow**：このトンネル グループへのトラフィックを優先トラフィックに設定します。
- **Police output**：このトンネル グループに向かうトラフィックをポリシングするための基準を確立します。このオプションをイネーブルにする場合は、認定レート、バースト レート、準拠アクション、および超過アクションの値を変更するか、デフォルト値を受け入れます。これらのパラメータの定義を参照する場合は、**Help** をクリックしてください。

ステップ 9　このトンネル グループのプライオリティ キューイングを確立するには、**Enable Priority for this flow** および **Finish** をクリックします。

ステップ 10　**Apply** をクリックします。

図 6-6 は、この例で設定された QoS セキュリティ ポリシーを示しています。

図 6-6　設定された QoS ポリシー



CLI コマンドを使用した手順

show running-config all service-policy コマンドを入力すると、特定のグループ ポリシーの実行サービス ポリシー コンフィギュレーションを表示できます。

次のコマンド例は、CLI を使用してトンネル グループの優先トラフィックを設定する方法を示しています（コマンド シーケンスが前の項で説明したウィザードと異なるので、注意してください）。

```
class-map outbound-class
  match tunnel-group 10.10.4.108
  match flow-ip destination-address
policy-map outbound policy
  class outbound-class
    priority
service-policy outbound-policy interface test
```

（注）　CLI を使用して QoS を設定する方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。