Configuring Traffic Management

This chapter describes the following configuration tasks:

Configuring Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected on the same network to handle remote sessions, you can configure those devices to share their session load. This feature is called *load balancing*. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides high availability.

To implement load balancing, group together logically two or more devices on the same subnet into a *virtual cluster.*

All devices in the virtual cluster carry session loads. One ASA in the virtual cluster, the *virtual cluster master*, can accept connections and also direct incoming calls to the other devices, called *backup devices*. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly. The role of virtual cluster master is not tied to a physical device; it can shift among devices. For example, if the current virtual cluster master fails, one of the backup devices in the cluster takes over that role and immediately becomes the new virtual cluster master.

To outside clients, the virtual cluster appears as a single *virtual cluster IP address*. This IP address is not tied to a specific physical device. It belongs to the current virtual cluster master; hence, it is virtual. A VPN client attempting to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available device in the cluster. In a second transaction (transparent to the user), the client connects directly to that device. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

If a device in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to an active device in the cluster. Should the virtual cluster master itself fail, a backup device in the cluster immediately and automatically takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

Note For load balancing to work for WebVPN, all devices in the cluster must support WebVPN.

Prerequisites

Load balancing is disabled by default. You must explicitly configure and enable it.

Before you can configure load balancing, the public and private interfaces must be configured and the interface for the virtual cluster IP address must be defined.

All devices in the cluster must share the same cluster-specific values:

- Virtual cluster IP address
- Encryption settings (optional)
- Encryption key (optional unless Encryption is enabled)
- Port identifier (the default UDP is 9023)

Overview of Configuration Procedure

To configure a minimal VPN load balancing scheme:

1. Define the virtual cluster IP address, the IP address to be shared by all devices in the VPN load balancing cluster. The address must be within the public subnet address range shared by the devices.
2. If configuring stateful failover, enable encryption and define an encryption key to be shared by all devices in the cluster. The devices in the virtual cluster communicate via LAN-to-LAN tunnels using IPSec. Enabling encryption ensures that all load-balancing information communicated between them is encrypted.
3. Optionally change the default priority of a device within the cluster. The range is from 1 to 10; 10 is the highest. The priority indicates the likelihood of the device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority, the more likely this device becomes the virtual cluster master.
4. Enable load balancing on each ASA included in the cluster.

The example in this section configures the following values:

- Cluster IP address is 209.165.202.224.
- Cluster encryption key is 12345678.
- Encryption is enabled on this cluster.
- The ASA in this example has a priority of 10.

The example in this section uses the following CLI commands to configure load balancing.

```
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
```

Using CLI Commands

You can enter the **show running-config vpn load-balancing** command to display the running configuration for a particular group policy.

Use the CLI to configure load balancing as follows:

Step 1 When you execute the **vpn load-balancing** command, the CLI puts you in config-load-balancing mode, where you configure the cluster parameters. In this mode, enter the **cluster** command to configure the virtual cluster IP address, as follows:

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

Step 2 To use encryption in this configuration, use **cluster** commands to define the encryption key and then enable encryption. This step is optional. You must configure the encryption key before you enable encryption.

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

Step 3 (Optional) To change the default priority of the ASA, use the **priority** command, as follows:

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

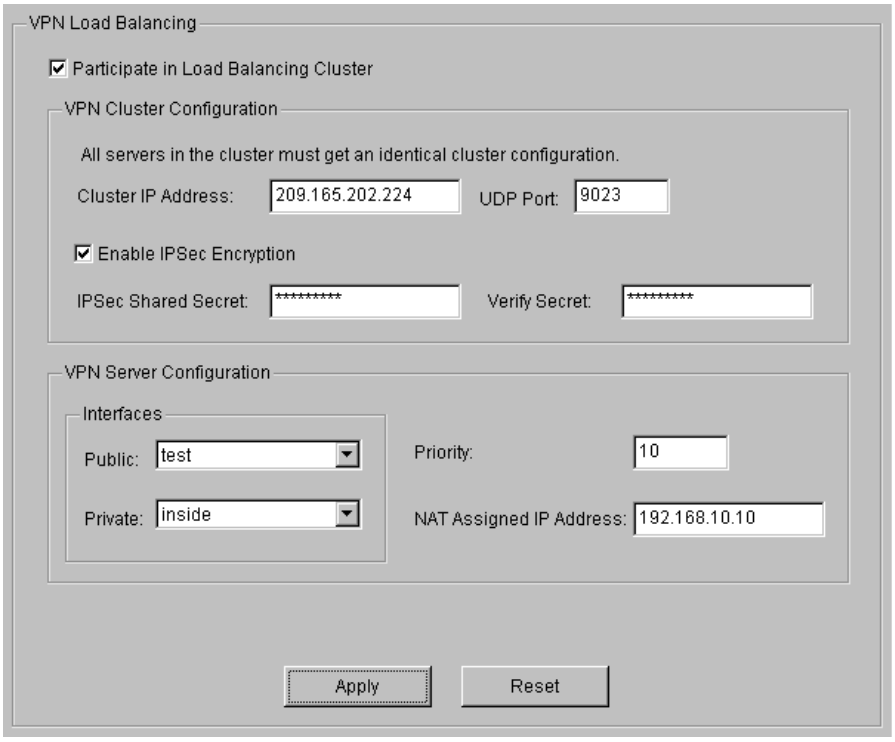
Step 4 To enable load balancing on this ASA, use the **participate** command, as follows:

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

Using ASDM

The following procedure shows how to use ASDM to configure load balancing. Note that many of the parameters in this example have default values.

Figure 6-1 Configuring Load Balancing in ASDM



Step 1 To enable VPN load balancing, go to **Configuration > Features > VPN > Load Balancing**, and click **Participate in Load Balancing Cluster**.

Step 2 In the **VPN Cluster Configuration** group box, configure the parameters for all ASAs participating in the cluster, as follows:

- **a.** Type the IP address of the cluster in the **Cluster IP Address** text box.
- **b.** Click the **Enable IPSec Encryption** option.
- **c.** Type the encryption key in the **IPSec Shared Secret** text box and type it again in the **Verify Secret** text box.

Step 3 Configure the options in the **VPN Server Configuration** group box:

- **a.** In the **Public** list, select an interface that will accept the incoming VPN connections.
- **b.** In the **Private** list, select an interface that is the private interface.
- **c.** (Optional) Change the priority that the ASA has in the cluster in the **Priority** text box.
- **d.** If this device is behind a firewall using NAT, type an IP address for the **NAT Assigned IP Address**. For this example, the NAT assigned IP address is 192.168.10.10. If the device is not using NAT or if the ASAs are not behind a firewall using NAT, enter 0.0.0.0.

Configuring Quality of Service for VPN Traffic

The VPN 3000 Concentrator implemented bandwidth management as a part of traffic policy management. QoS, a component of the security policy configuration of the ASA, supersedes that implementation. In the ASA, the implementation of QoS is based on the IOS implementation of that feature.

QoS is a traffic-management strategy that lets you allocate network resources for both mission-critical and normal data, based on the type of network traffic and the priority you assign to that traffic. In short, QoS ensures unimpeded priority traffic or provides the capability of rate-limiting (policing) traffic.

QoS provides maximum rate control, or policing, on each individual user tunnel and site-to-site tunnel. (Individual user traffic within a tunnel is not taken into consideration for LAN-to-LAN connections.) This release does not provide a minimum bandwidth guarantee (bandwidth reservation).

Because QoS can consume large amounts of resources, which could degrade ASA performance, QoS is disabled by default.

The following sections show briefly how to use QoS to configure priority traffic for tunnel groups only.

Note Refer to *Cisco Security Appliance Command Line Configuration Guide* for complete information about QOS.

Overview of Configuration Procedure

Use ASDM to configure QoS as follows:

1. Configure a service policy.

   There can be only one service policy per interface or at the global level.
2. Configure the traffic classification criteria for the service policy rule.
3. Configure actions on the traffic classified by the service policy rule.

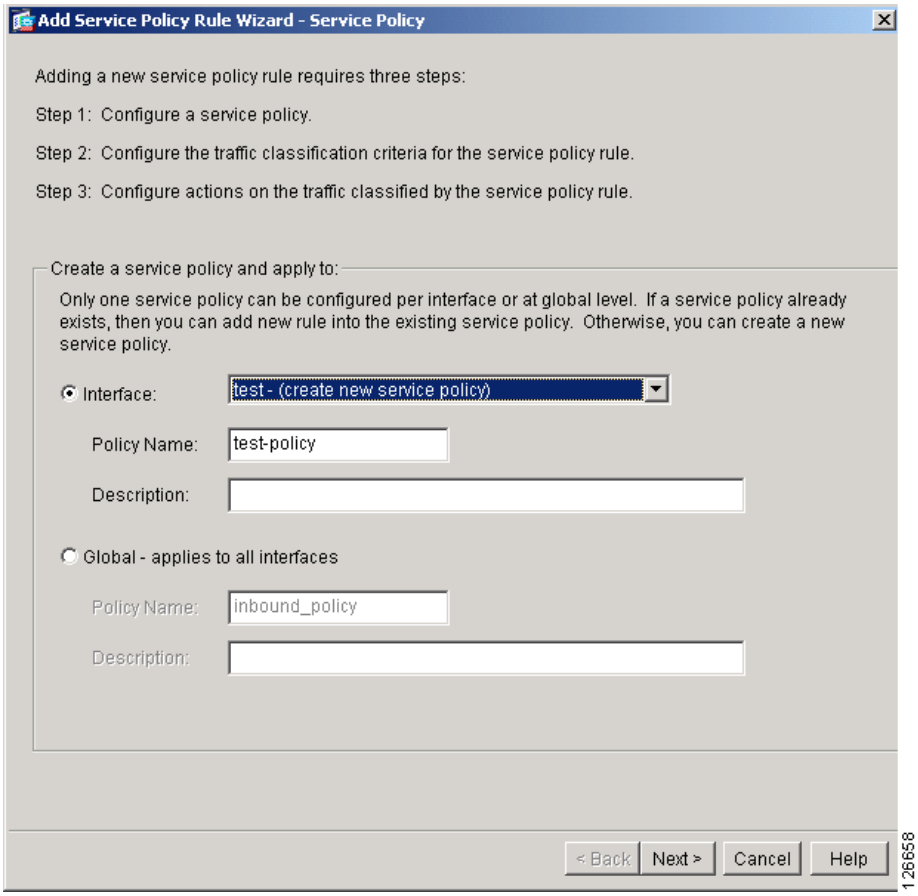
Using ASDM

ASDM provides a wizard to guide you through the steps for configuring QoS. This section shows how to use this wizard to configure QoS for a tunnel group. The ASDM **Help** button provides additional information.

Step 1 Under the **Configuration > Features > Security policy** panel, click **Service Policy Rules**.

Step 2 Click **Add**. ASDM displays the **Add Service Policy Rule Wizard - Service Policy** dialog box. Use this dialog box to create or edit a service policy.

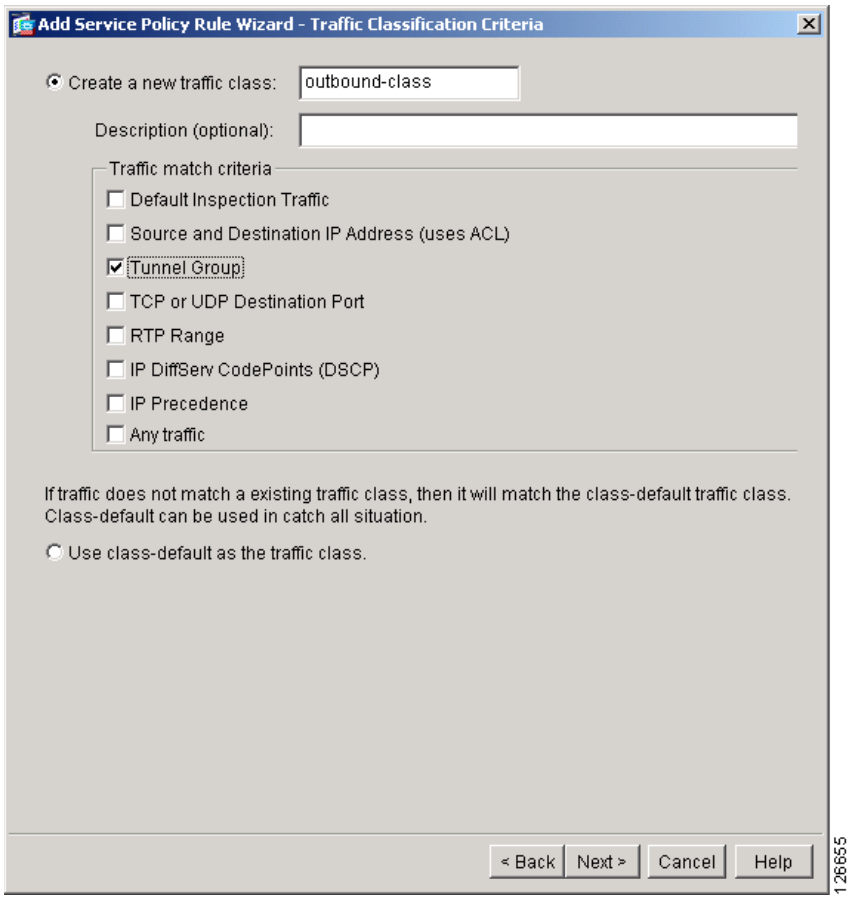
Figure 6-2 **Add Service Policy Rule Wizard - Service Policy Wizard**



Step 3 This example creates a new service policy and applies it to the test interface. To start, click the **Interface** option and then select the name **test - (create new service policy)** from the **Interface** list. (The text (create new service policy) is appended to the name of the interface).

Step 4 Type a name for the policy in the **Policy Name** text box. ASDM provides a default name by appending the word "policy" to the interface name. For this example, change it to outbound-policy. Click **Next**. ASDM displays the **Add Service Policy Rule Wizard - Traffic Classification Criteria** dialog box.

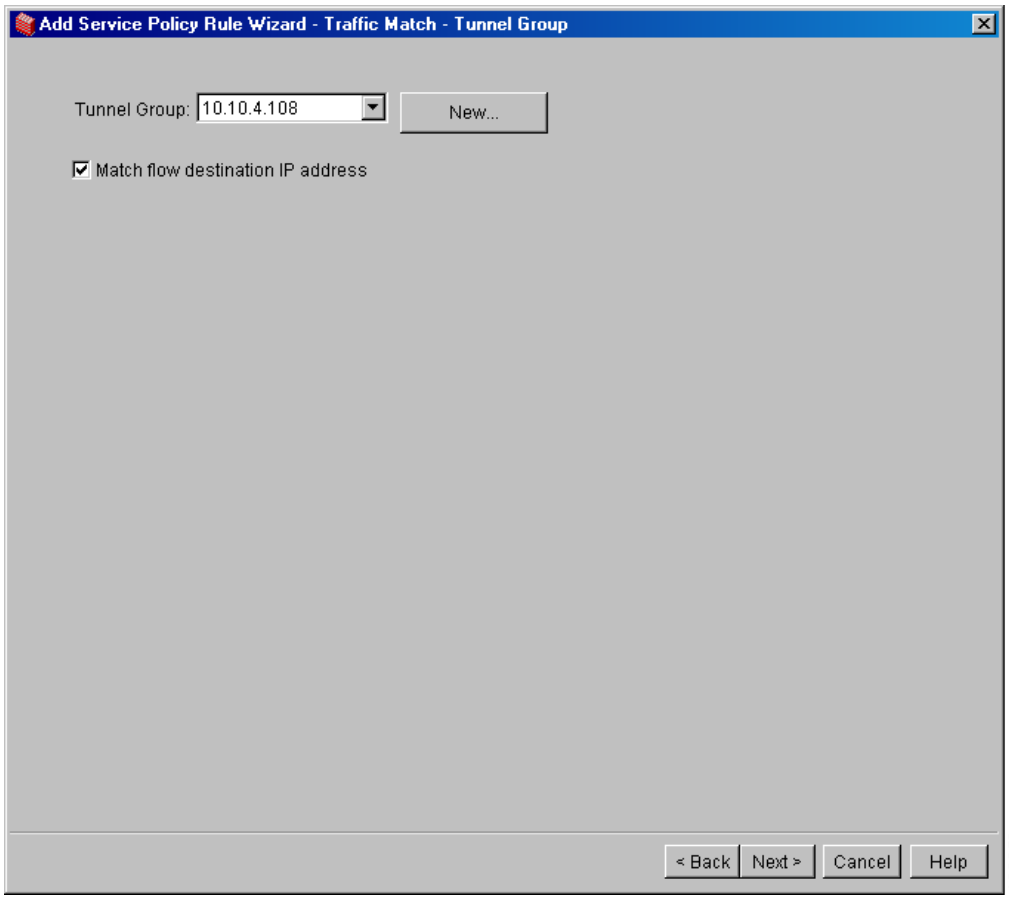
Figure 6-3 Add Service Policy Rule Wizard - Traffic Classification Criteria



Step 5 Click the **Create a new traffic class** option. ASDM combines the interface name with the word "class" to create a default policy name in the text box. For this example, change the name to outbound-class.

Step 6 The **Traffic match criteria** group box displays a subset of the match criteria that the ASA offers. For this example, click the **Tunnel Group** option and click **Next**. ASDM displays the **Add Service Policy Rule Wizard-Traffic Match - Tunnel Group** dialog box.

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

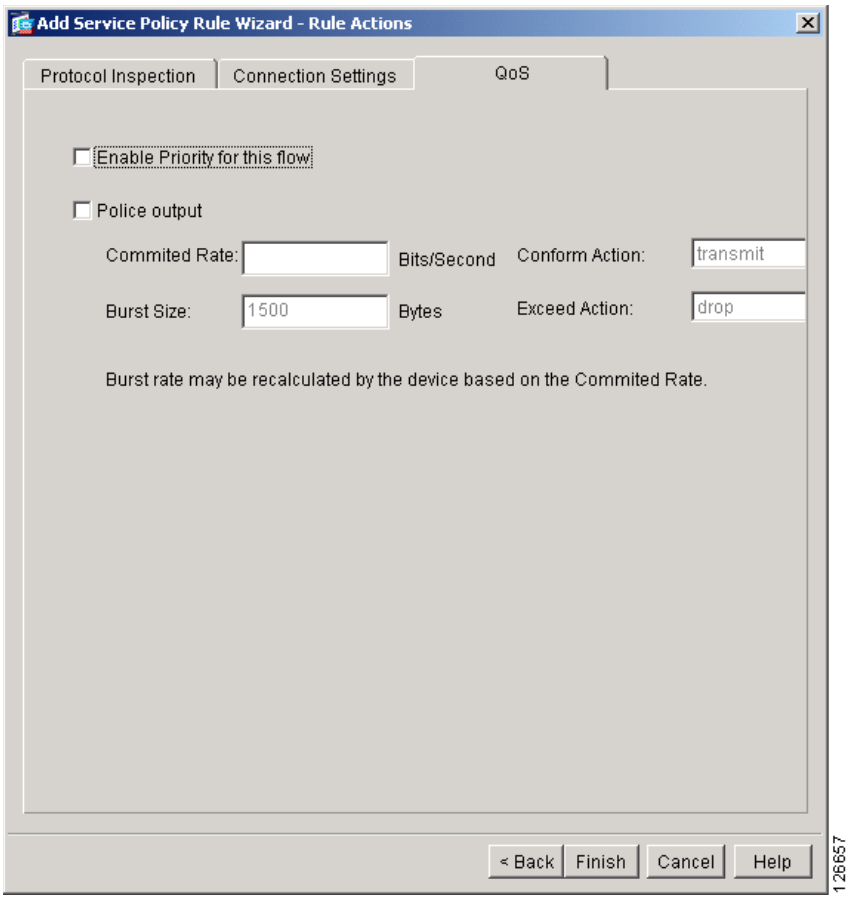


Step 7 Select the IP address of a tunnel group already in the system or click **New** to configure a new tunnel group. For this example, select an **10.10.4.108** from the **Tunnel Group** list and click **Match flow destination IP address**. Enabling this option applies the traffic action to be selected in the next dialog box to this tunnel group. Click **Next**.

ASDM displays the **Add Service Policy Rule Wizard - Rule Actions** dialog box.

Step 8 Click the **QoS** tab.

Figure 6-5 Configuring QoS Options



The QoS tab lets you select one of the following rule actions:

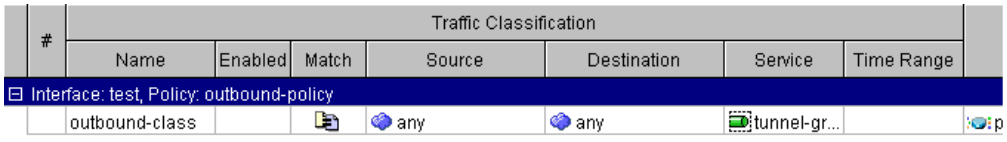
- **Enable Priority for this flow**—Make traffic to this tunnel-group a priority.
- **Police output**—Establish criteria for policing the traffic going to this tunnel group. If you enable this option, change the values for committed rate, burst rate, conform action and exceed action, or accept the default values. For definitions of these parameters, click **Help**.

Step 9 To establish priority queuing for this tunnel group, click **Enable Priority for this flow** and **Finish**.

Step 10 Click **Apply**.

Figure 6-6 shows the QoS security policy configured for this example.

Figure 6-6 QoS Policy Configured



Using CLI Commands

You can enter the **show running-config all service-policy** command to display the running service policy configuration for a particular group policy.

The following commands provide an example of how to use the CLI to configure priority traffic for tunnel groups. (Note that the command sequence is different from the wizard described in the previous section.)

```
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
```

Note For detailed instructions on how to configure QoS with the CLI, see *Cisco Security Appliance Command Line Configuration Guide*.