Pulse Secure®

Load-Balancing Pulse Connect Secure with Pulse Secure Virtual Traffic Manager

Deployment Guide

Published 15 November, 2019

Document Version 1.5

Pulse Secure
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Load-Balancing Pulse Connect Secure with Pulse Secure Virtual Traffic Manager

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

INTRODUCTION 1
Purpose of this Guide 1
Prerequisites 1
The Challenge 1
The Solution 2
Configuration Summary 2

CONFIGURING PULSE CONNECT SECURE AS AN ACTIVE-ACTIVE CLUSTER PAIR 3

CONFIGURING THE TRAFFIC MANAGER 9
Using the Load-balance Pulse Connect Secure Wizard 10
Configuring the Traffic Manager Manually 16
Creating a Traffic IP Group 17
Creating an IP-based Session Persistence Class 18
Creating PCS Pools 19
Configuring Virtual Servers in the Traffic Manager 21
Starting your Services 24
Optional: Configuring IP Transparency 25
Optional: Weighted Load Balancing with Service Discovery 28
Configuring PCS to Accept Healthcheck Requests 28
Configuring the Traffic Manager to use the Healthcheck API 28

VERIFYING OPERATION 31

Introduction

Purpose of this Guide

This guide describes how to configure Pulse Secure Virtual Traffic Manager (the Traffic Manager) to load balance VPN connections to an active-active Pulse Connect Secure (PCS) cluster.

Prerequisites

This guide assumes you are familiar with the operation and administration of Pulse Connect Secure and Pulse Secure Virtual Traffic Manager.

This guide does not cover the initial installation tasks associated with setting up PCS or the Traffic Manager. The steps referred to in this guide assume you have a fully working and licensed set of PCS and Traffic Manager instances, and that your Traffic Managers are joined in a fault-tolerant cluster.

Note: While the Traffic Manager can operate as a singular instance, Pulse Secure recommends you deploy a cluster of two or more Traffic Manager instances for full fault-tolerance and failover in the event of service disruption. References to *the* Traffic Manager throughout this guide should be understood to refer to the configuration shared across all Traffic Manager instances.

For details of how to create a Traffic Manager cluster, see the *Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide* applicable to your product variant.

The Challenge

PCS supports two types of clusters:

- Failover clusters (also known as active/passive clusters)
- Load balancing clusters (also known as active/active clusters)

Failover clusters provide high-availability. If the active machine is unable to provide a service, the passive machine takes over hosting the service. Failover clusters require only a single IP address to operate and so do not require load-balancing functionality, however they are limited to operating in pairs and cannot scale if the number of users exceeds the capacity of a single PCS server.

Load balancing clusters address these limitations by allowing up to four PCS servers to be joined in an active/active deployment model. All the PCS servers in the cluster can actively handle user sessions, and if one should fail the user can connect to a different server to resume their session.

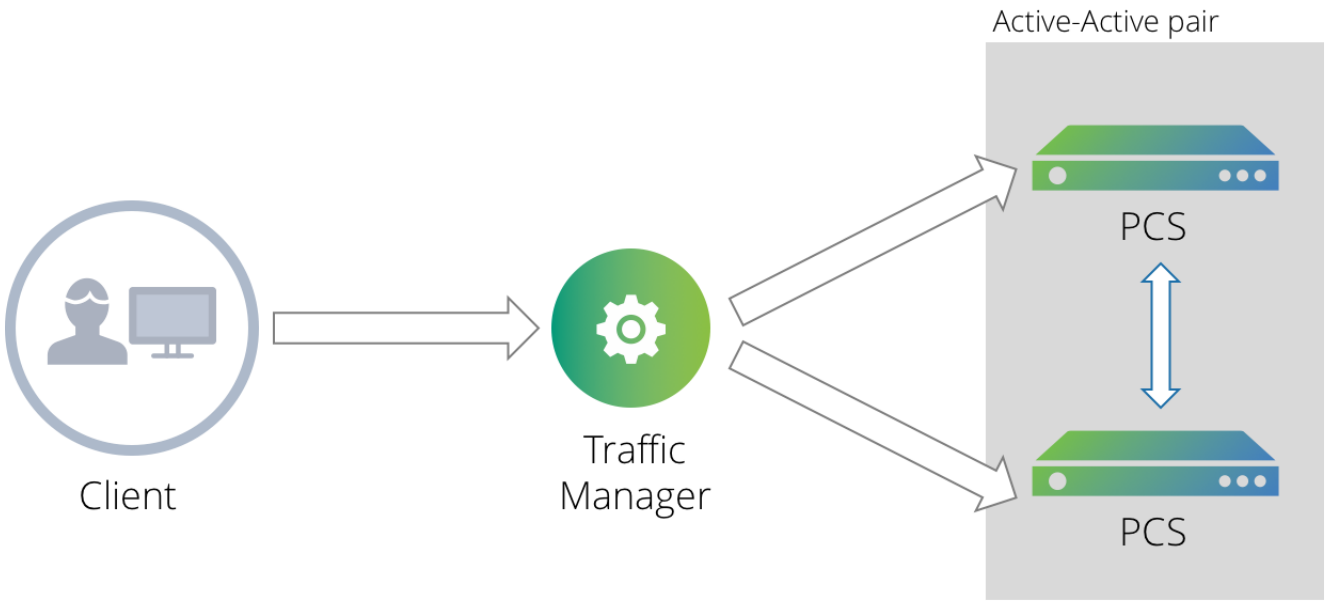
Load balancing clusters require an external device to distribute incoming user sessions between the active PCS servers. The load-balancing device must be able to evenly distribute user sessions across the PCS servers and monitor the health of the servers so users can be directed away from a failed cluster member.

The Solution

Pulse Secure Virtual Traffic Manager provides the all the necessary capabilities to load balance incoming user sessions across an active-active PCS cluster based on the health of each PCS instance and, optionally, the number of free license seats remaining.

This deployment guide describes how to configure your PCS servers to function as an active-active cluster, and then how to configure the Traffic Manager with a load-balancing service to distribute user session load across the cluster.

Figure 1 Load-balancing traffic across a pair of PCS instances



Configuration Summary

To apply load-balancing across your PCS instances, perform the following steps:

1. Configure your PCS instances as an active-active cluster pair.
2. Configure the Traffic Manager with UDP (Streaming) and SSL services, directed at your PCS cluster.
3. Optionally, add weighted load balancing based on the detected free license capacity on each PCS instance.

The remainder of this guide describes each of these steps in detail.

Configuring Pulse Connect Secure as an Active-Active Cluster Pair

Before you begin, make sure the following conditions are met:

- Your Pulse Connect Secure (PCS) instances are installed and configured in the same subnet
- All PCS instances run the same software version
- All PCS instances use the same hardware platform
- Your Pulse Secure Virtual Traffic Manager (Traffic Manager) instance is installed, configured for basic operation, and visible to your PCS instances

To create an active-active PCS cluster pair, perform the following steps:

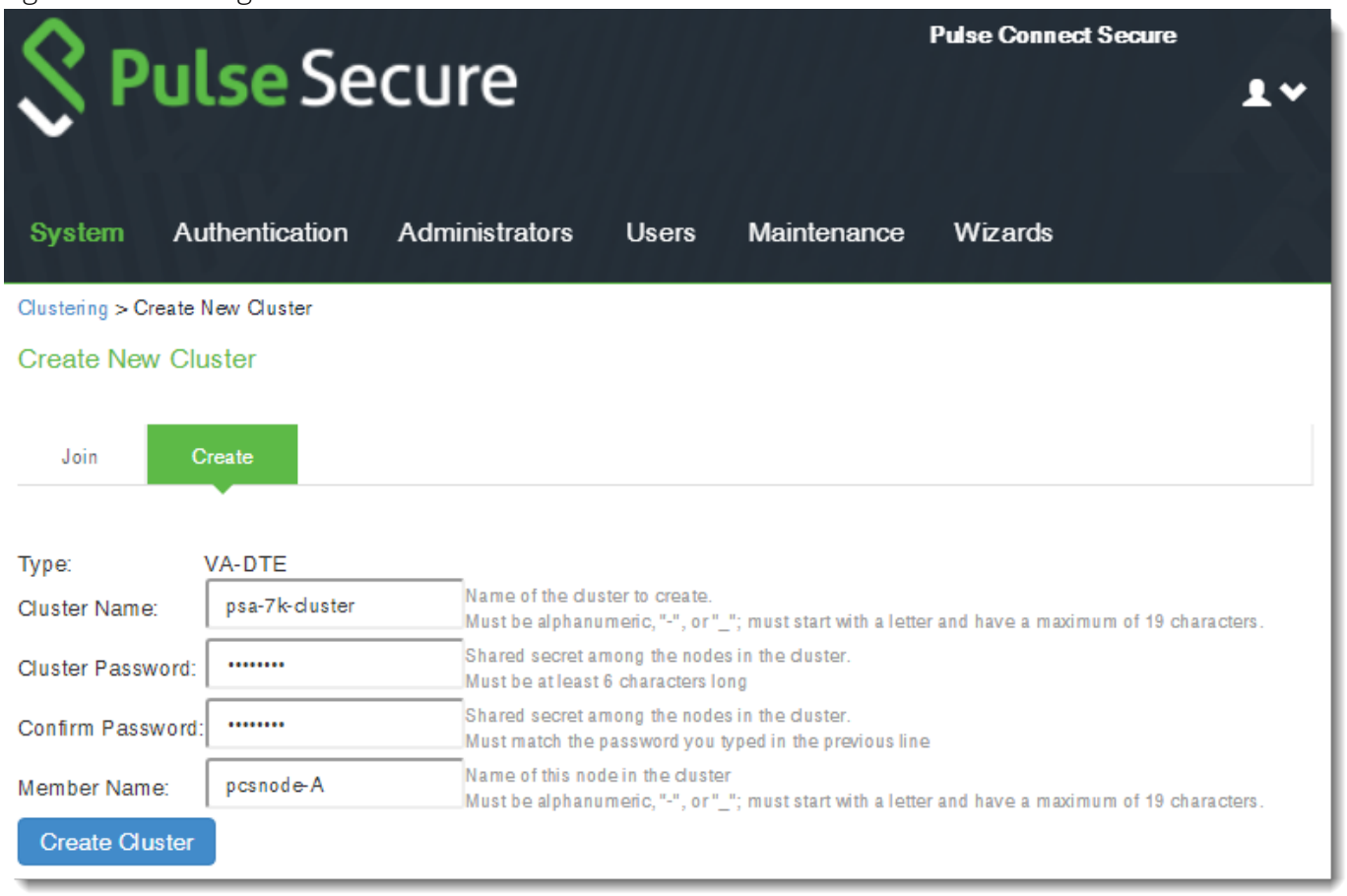
1. Login to the Admin UI on one of your PCS instances.

   Note: Choose the instance that you want to designate as the "leader" for the cluster. The leader instance replicates its own configuration out to any other PCS instances you join to the cluster.

2. Click **System > Clustering > Create Cluster** and type a name for the cluster, a cluster password, and a name for this cluster instance.

   All instances that you join to the cluster use the password you specify here for administration and internal communication.

Figure 2 Creating a new PCS cluster

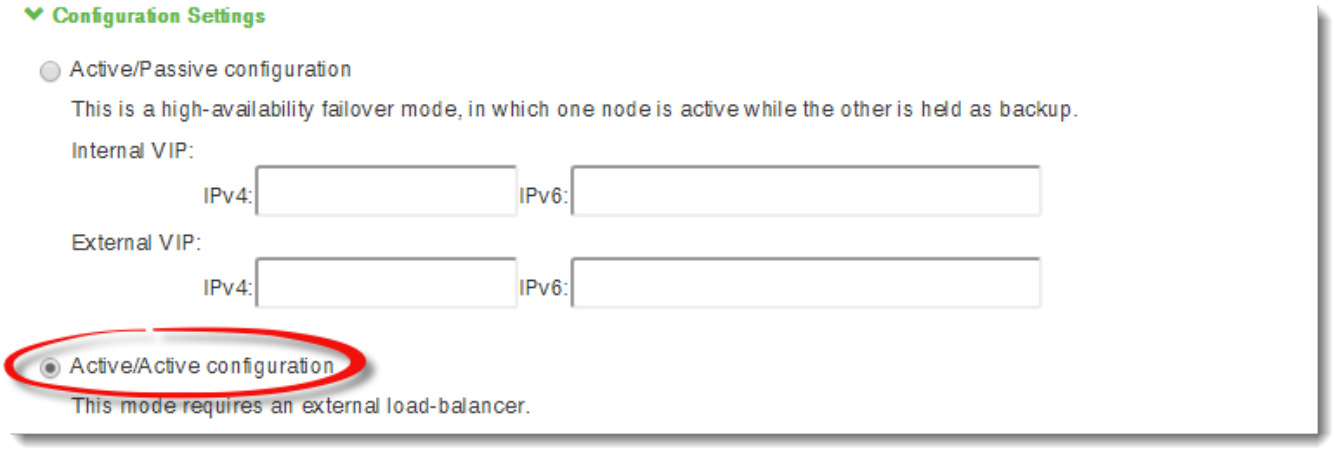


3. To create the new cluster, click **Create Cluster**. When prompted to confirm cluster creation, click **Create**.

   After PCS initializes the cluster, the Clustering page displays **Status** and **Properties** tabs.

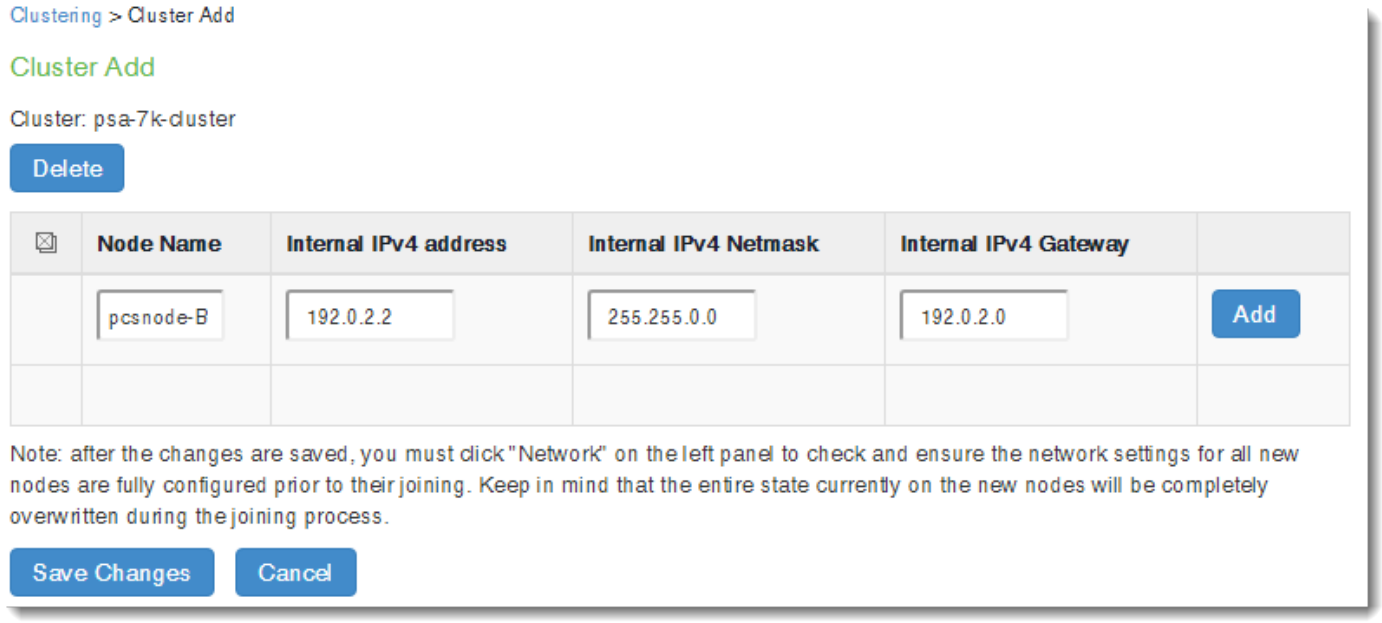
4. In the **Properties** tab, locate the "Configuration Settings" section and make sure "Active/Active Configuration" is selected. To save any updates, click **Save Changes**.

Figure 3 Setting Active/Active cluster configuration



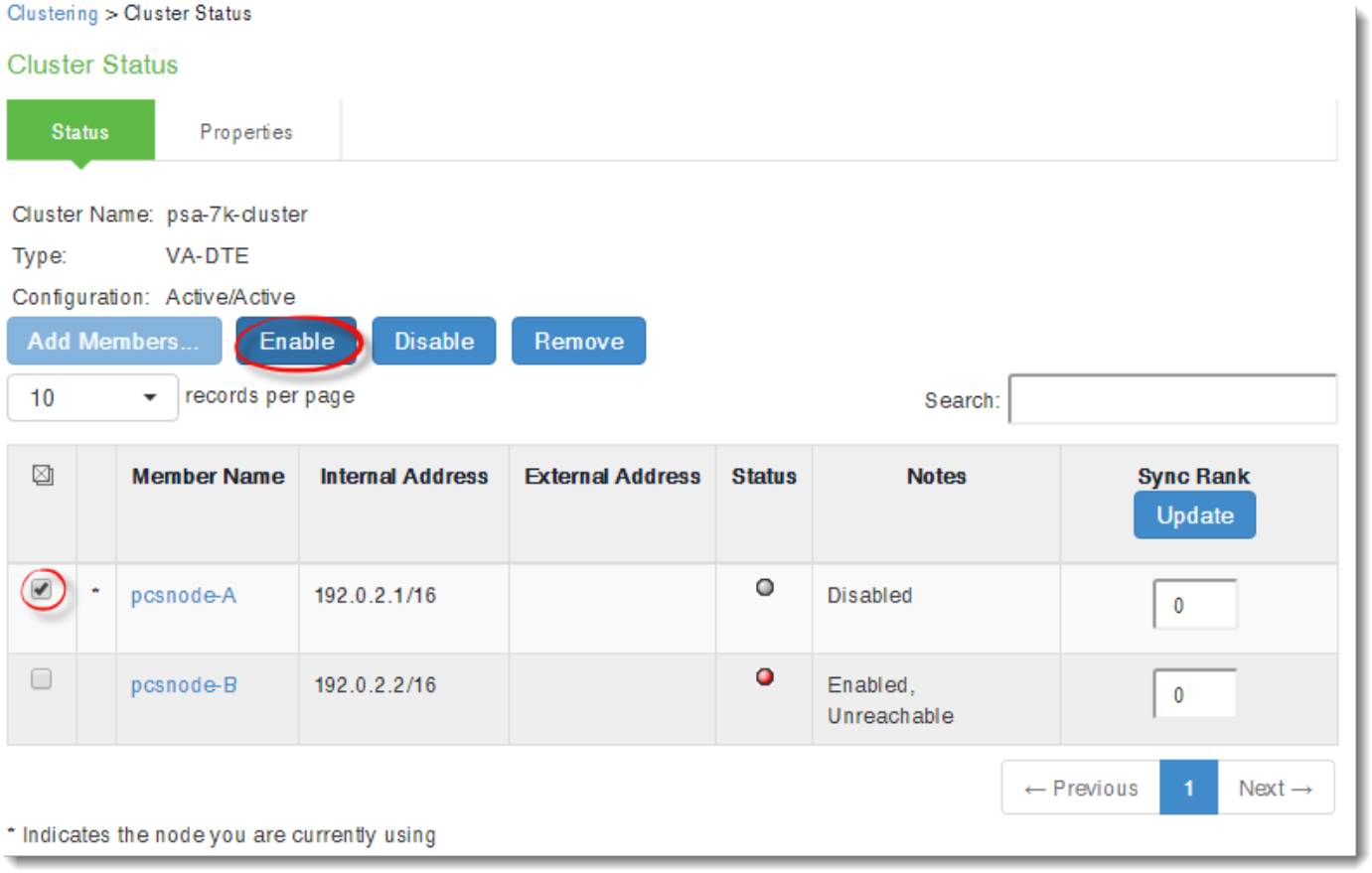
5. To join an additional PCS instance to the cluster, select the **Status** tab and then click **Add Members**.
6. Specify the joining instance name, IPv4 address, netmask, and internal gateway. To add the specified instance to the cluster, click **Add** and then click **Save Changes**.

Figure 4 Adding a cluster member



7. Your first PCS instance must be enabled before you can complete the remaining steps. If the PCS instance is not enabled automatically, enable it manually on the **Status** tab by ticking the corresponding checkbox and clicking **Enable**. On the confirmation page that follows, click **Enable**.

Figure 5 Manually enabling the leader PCS instance



8. Next, login to the Admin UI on the second PCS instance, and navigate to **System > Clustering > Cluster Join**.
9. Type the name and password of the cluster you want this PCS instance to join, and specify the IP address of the PCS instance on which you just created the named cluster. Click **Join Cluster** to begin the process, then click **Join** on the confirmation page that follows.

Figure 6 Joining a cluster defined on another PCS instance

Note: For further information on PCS cluster configuration, refer to the Clustering section of the *Pulse Connect Secure Administration Guide*.

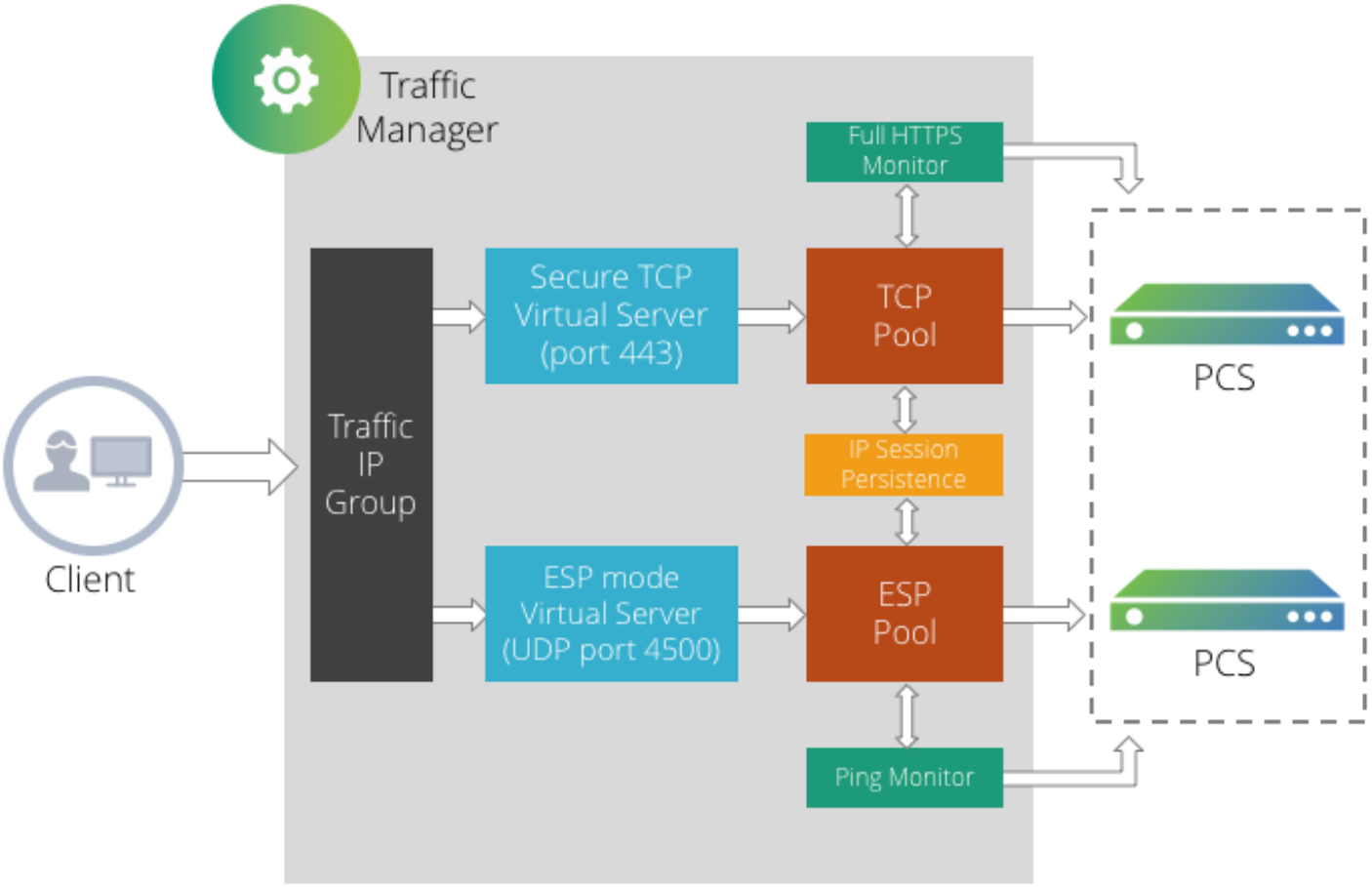
To confirm the status of your cluster, and the assigned internal and external interfaces, click **System > Clustering > Status**. Observe the "Status" and "Notes" fields alongside each cluster member for indications of any unresolved communication issues.

Configuring the Traffic Manager

When a client attempts to establish a VPN session with Pulse Connect Secure (PCS), it starts by creating a secure TCP control connection. After authenticating over this connection, the client then attempts to send ESP traffic over a secure UDP channel. As such, Pulse Secure Virtual Traffic Manager (the Traffic Manager) must be configured to receive both types of traffic and must load-balance both TCP and ESP traffic originating from the same client to the same PCS instance.

In the event that a secure UDP channel cannot be established between the client and the PCS server, the client falls back to using the TCP connection for the VPN traffic.

Figure 7 Traffic Manager Configuration Overview



Pulse Secure Virtual Traffic Manager versions 18.2 and later include a wizard to create automatically all the required services to communicate with your PCS instances (see "Using the Load-balance Pulse Connect Secure Wizard" on page 10). For Traffic Manager versions earlier than 18.2, you must manually set up the Traffic Manager configuration illustrated above (see "Configuring the Traffic Manager Manually" on page 16).

Pulse Secure Virtual Traffic Manager versions 19.3 and later, in conjunction with Pulse Connect Secure versions 9.1R3 and later, include the optional capability to communicate the real-time number of free license seats available on each PCS instance. This information provides the Traffic Manager with enhanced load awareness and can help to ensure user sessions are more evenly distributed across the PCS cluster. To learn more about this capability, see "Optional: Weighted Load Balancing with Service Discovery" on page 28.

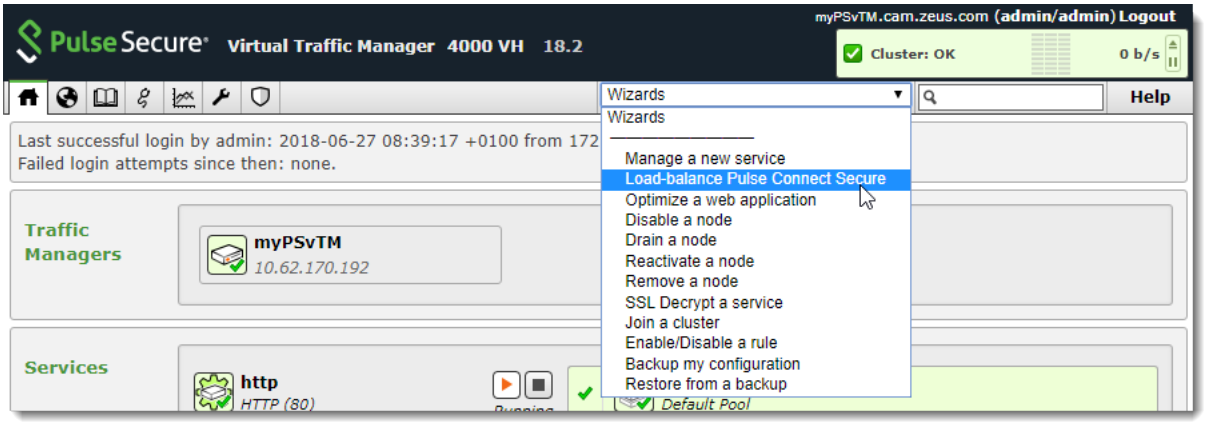
The remainder of this guide assumes that you have already created an active-active PCS cluster pair, as described in "Configuring Pulse Connect Secure as an Active-Active Cluster Pair" on page 3.

Using the Load-balance Pulse Connect Secure Wizard

Note: This section applies only to Traffic Manager versions 18.2 and later. For versions earlier than 18.2, see instead "Configuring the Traffic Manager Manually" on page 16.

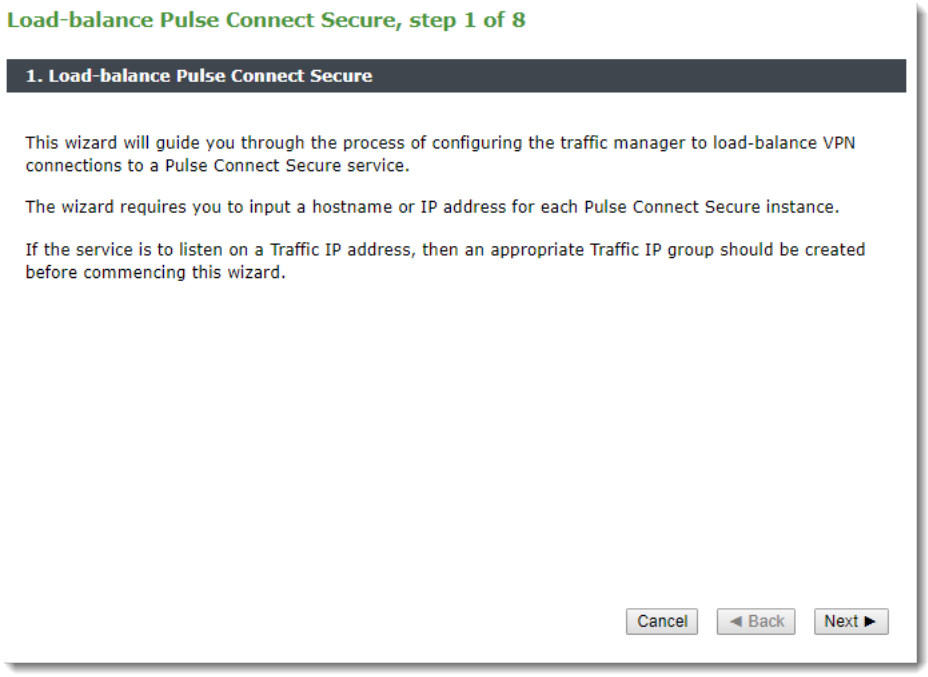
To run the wizard, click the "Wizards" drop-down menu in the tool bar, then select "Load-balance Pulse Connect Secure".

Figure 8 Running the "Load-balance Pulse Connect Secure" wizard



The Traffic Manager displays the first page of the wizard.

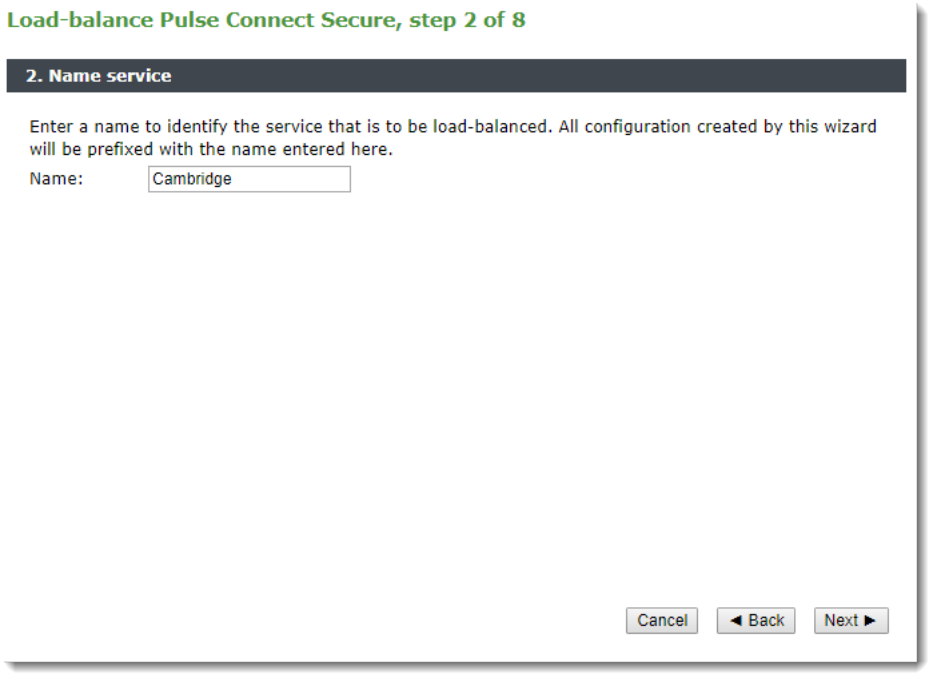
Figure 9 Starting the "Load balance a Pulse Secure cluster" wizard



Click **Next** to continue.

Note: Click **Cancel** at any time to cancel the wizard without making any changes. Use **Back** to return to the previous page and **Next** to continue on to the next page.

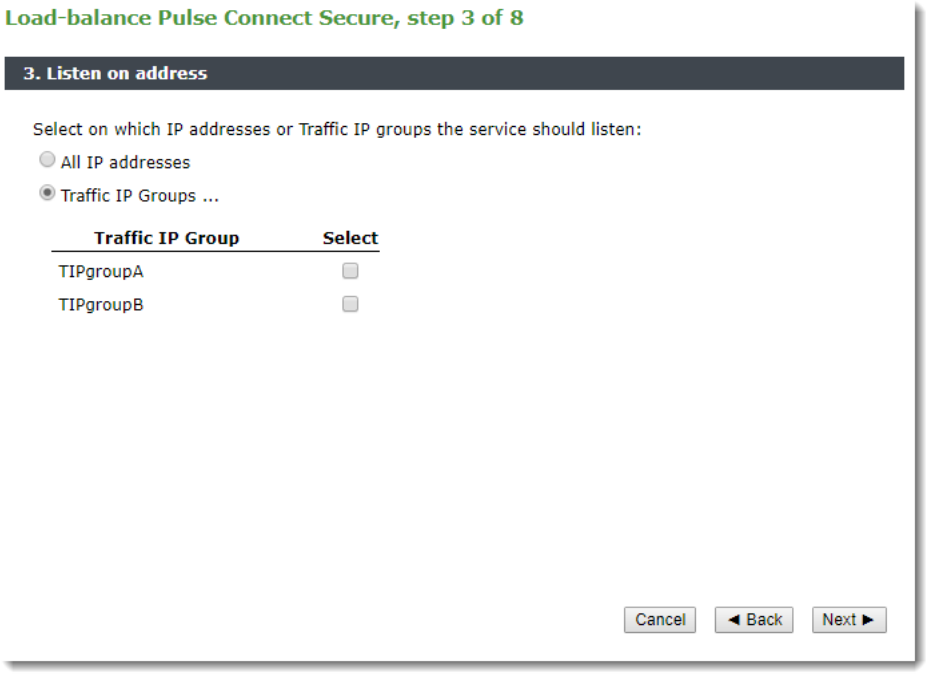
Figure 10 Providing an identifying name for the services



The Traffic Manager uses the identifier you provider here as a prefix for all configuration objects it creates through this process.

Type an identifying name and click **Next** to continue.

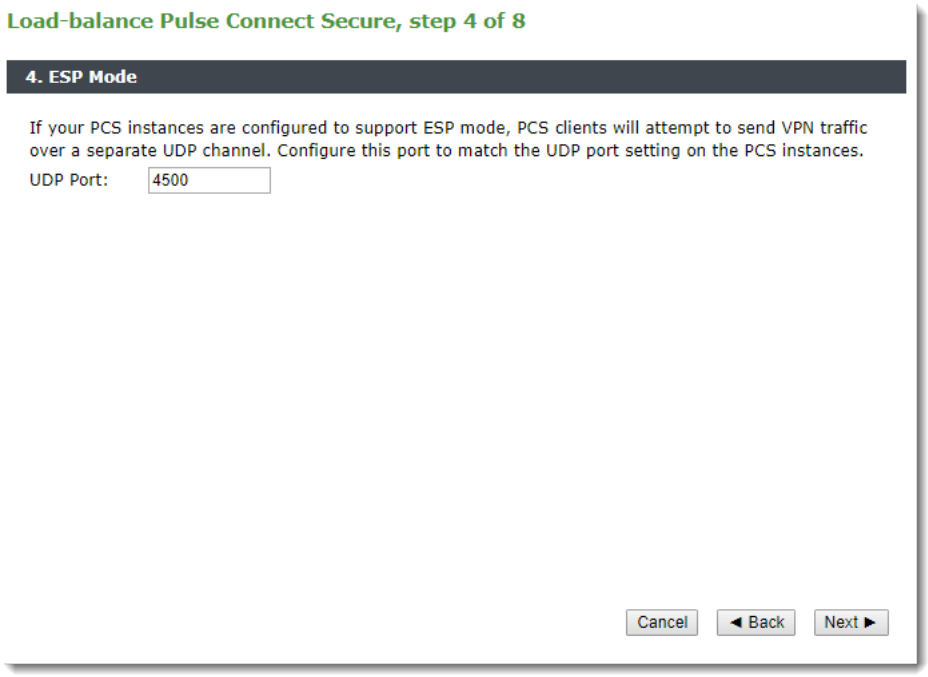
Figure 11 Specifying the IP addresses or Traffic IP groups this service should use



Use this page to determine if you want your VPN service to listen on all IP addresses hosted by the Traffic Manager, or to instead use a previously-defined Traffic IP group. To learn more about Traffic IP addresses and groups, see “Creating a Traffic IP Group” on page 17.

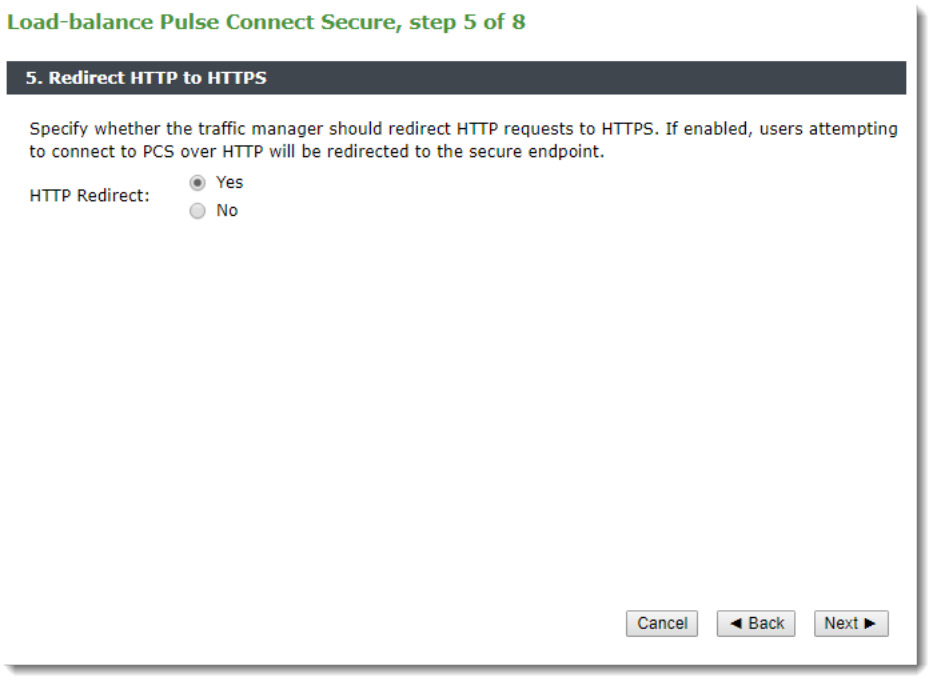
Select an option from the list and click **Next** to continue.

Figure 12 Specifying the UDP port number



The Traffic Manager uses the value you specify here to configure the ESP mode UDP streaming virtual server. Make sure the port number you specify matches the UDP port setting on your PCS instances.

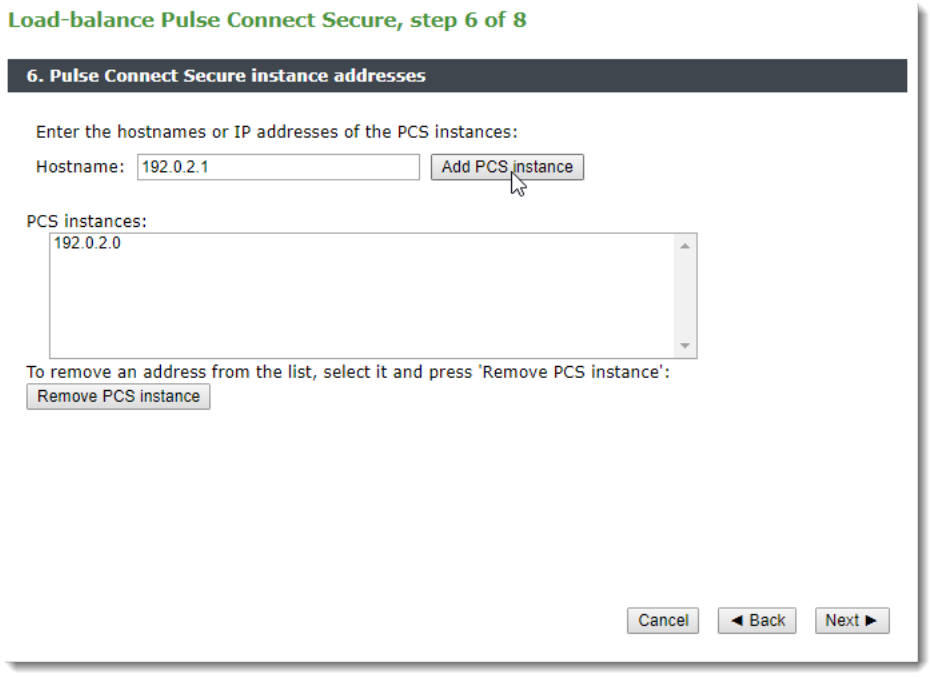
Figure 13 Configuring HTTP redirect



Use this setting to configure the Traffic Manager to ensure requests sent over HTTP are redirected to a secure HTTPS endpoint. Pulse Secure recommends consulting the network security policies of your organization before enabling this option.

Click **Next** to continue.

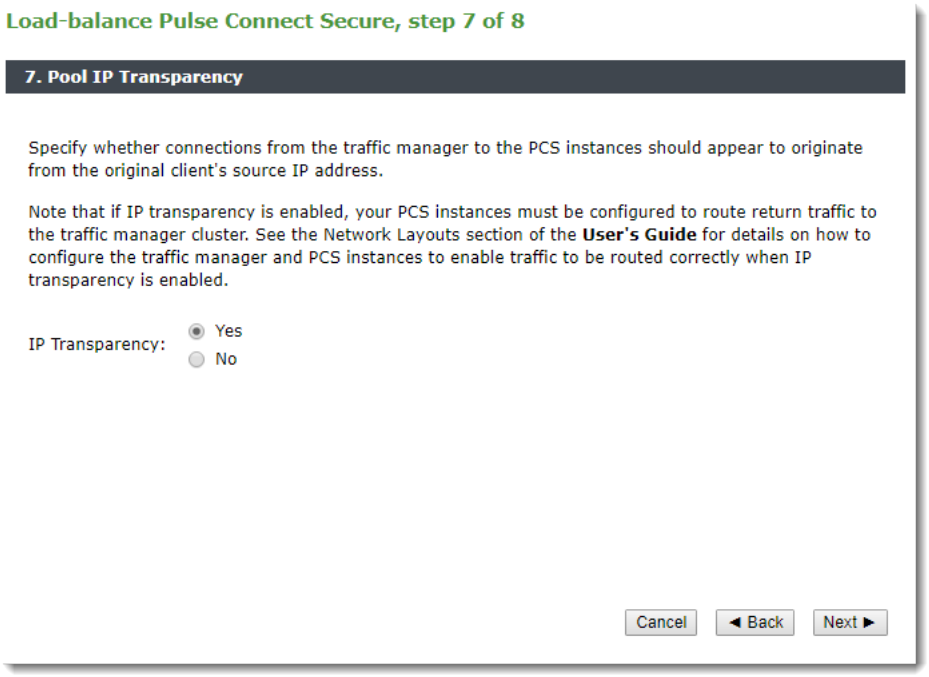
Figure 14 Adding PCS cluster members



Use this page to add your PCS cluster to the Traffic Manager. For each cluster member, type the hostname or IP address into the **Hostname** field and click **Add** PCS **instance** to add it to the list. To remove a PCS instance, select the corresponding list entry and click **Remove** PCS **instance**.

Click **Next** to continue.

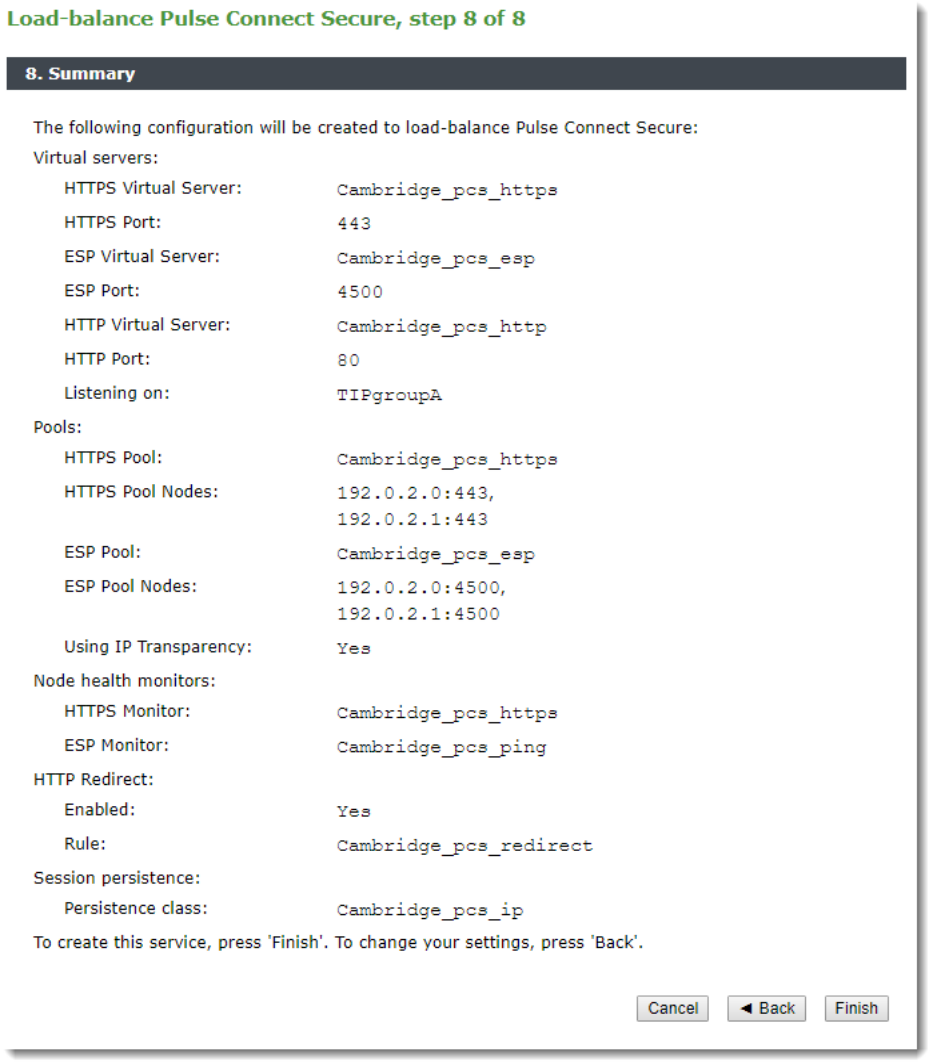
Figure 15 Configuring IP transparency



To enable IP transparency on the VPN service, set **IP transparency** to "Yes". To learn more about IP transparency, see "Optional: Configuring IP Transparency" on page 25.

Click **Next** to continue.

Figure 16 Summary of your settings



This page displays a summary of the proposed Traffic Manager settings. Click **Cancel** to quit the wizard without making any changes, click **Back** to return to the previous page, or click **Finish** to complete the wizard and configure the Traffic Manager.

After the wizard has completed all configuration, the Traffic Manager Home Page is updated to show all running services.

Configuring the Traffic Manager Manually

Use these steps to create or modify the individual configuration objects required by the Traffic Manager to load-balance a PCS cluster.

Note: This section is applicable to all supported versions of the Traffic Manager. For versions 18.2 and later, use *either* the Load-balance Pulse Connect Secure wizard, described in "Using the Load-balance Pulse Connect Secure Wizard" on page 10, or the individual steps described here.

Creating a Traffic IP Group

Permanent IP addresses assigned to the front-end network interfaces on your Traffic Managers are not suitable to use when you publish your VPN service. In the event of a hardware or system failure in your Traffic Manager cluster, your services would become partially or wholly unavailable.

The Traffic Manager's fault tolerance capability allows you to configure *Traffic IP addresses*. These IP addresses are not tied to individual Traffic Manager instances, and the cluster ensures that each IP address is fully available, even if some of the Traffic Manager instances have failed.

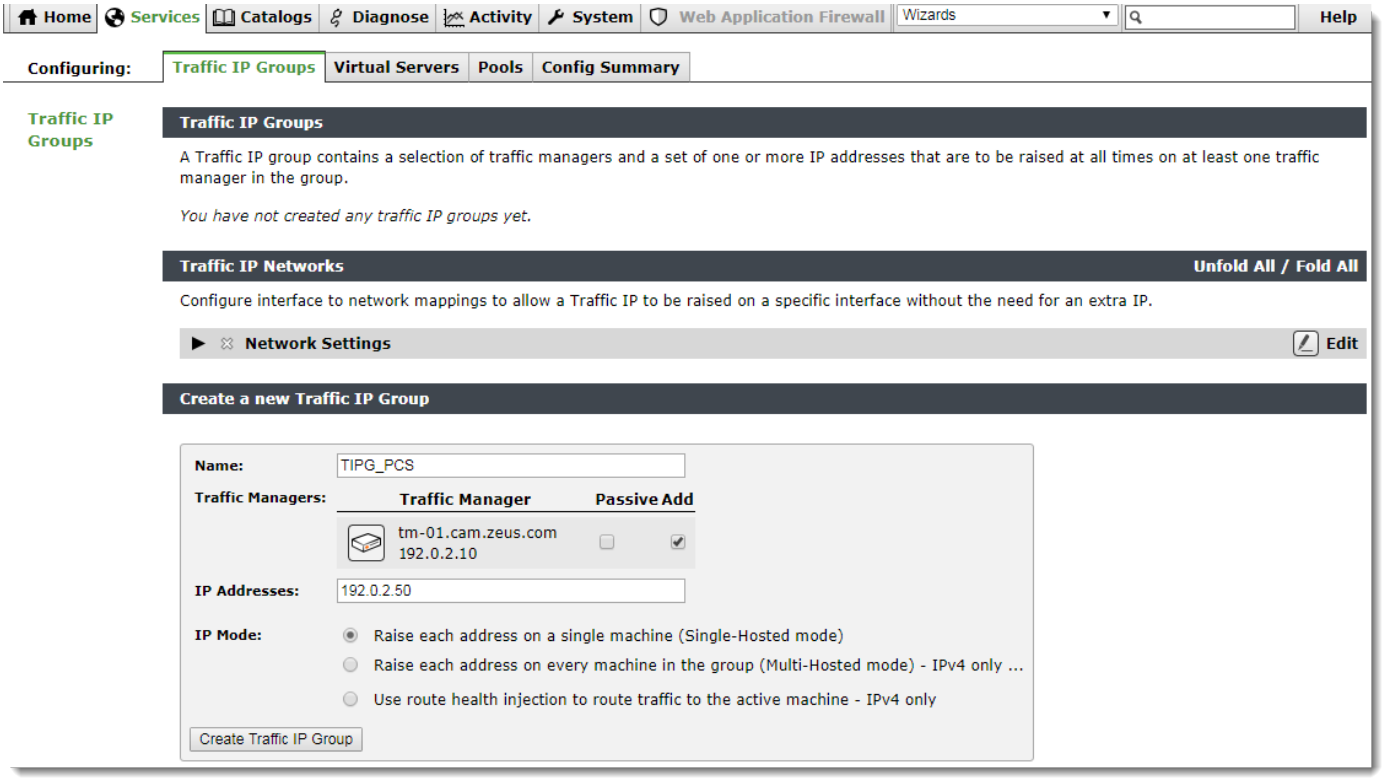
Traffic IP addresses are arranged into a Traffic IP group. You define the group as spanning some or all of your Traffic Manager instances. Group members negotiate between themselves to share out the traffic IP addresses, and each Traffic Manager then raises the IP address (or IP addresses) allocated to it.

To learn more about Traffic IP addresses and groups, see the "Traffic IP Groups and Fault Tolerance" chapter of the *Pulse Secure Virtual Traffic Manager: User's Guide*.

To create a Traffic IP Group, perform the following steps:

1. Login to the Traffic Manager Admin UI.
2. Click **Services > Traffic IP Groups**.
3. In the "Create a new Traffic IP Group" section, enter the details of your new Traffic IP Group:
    - **Name**: Type an identifying name for this group
    - Traffic Manager**s**: Select the Traffic Managers in your cluster you want to be members of the group
    - **IP Addresses**: Type the publicly-visible service IP addresses to be managed by this group, in a space- or comma-separated list
    - **IP Mode**: Choose the IP distribution mode for this group

Figure 17 Creating a Traffic IP Group



4. To create your group, click **Create Traffic IP Group**.

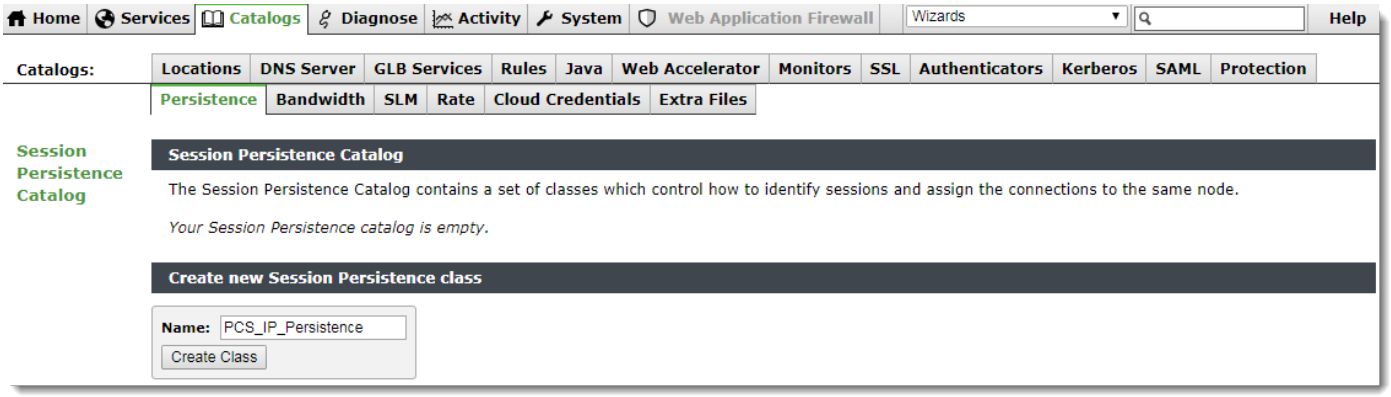
Creating an IP-based Session Persistence Class

To ensure that VPN traffic is sent to the same PCS instance that is handling the corresponding control connection, both TCP and ESP mode pools must have session persistence enabled, with the same persistence class shared between them.

To create a session persistence class, perform the following steps:

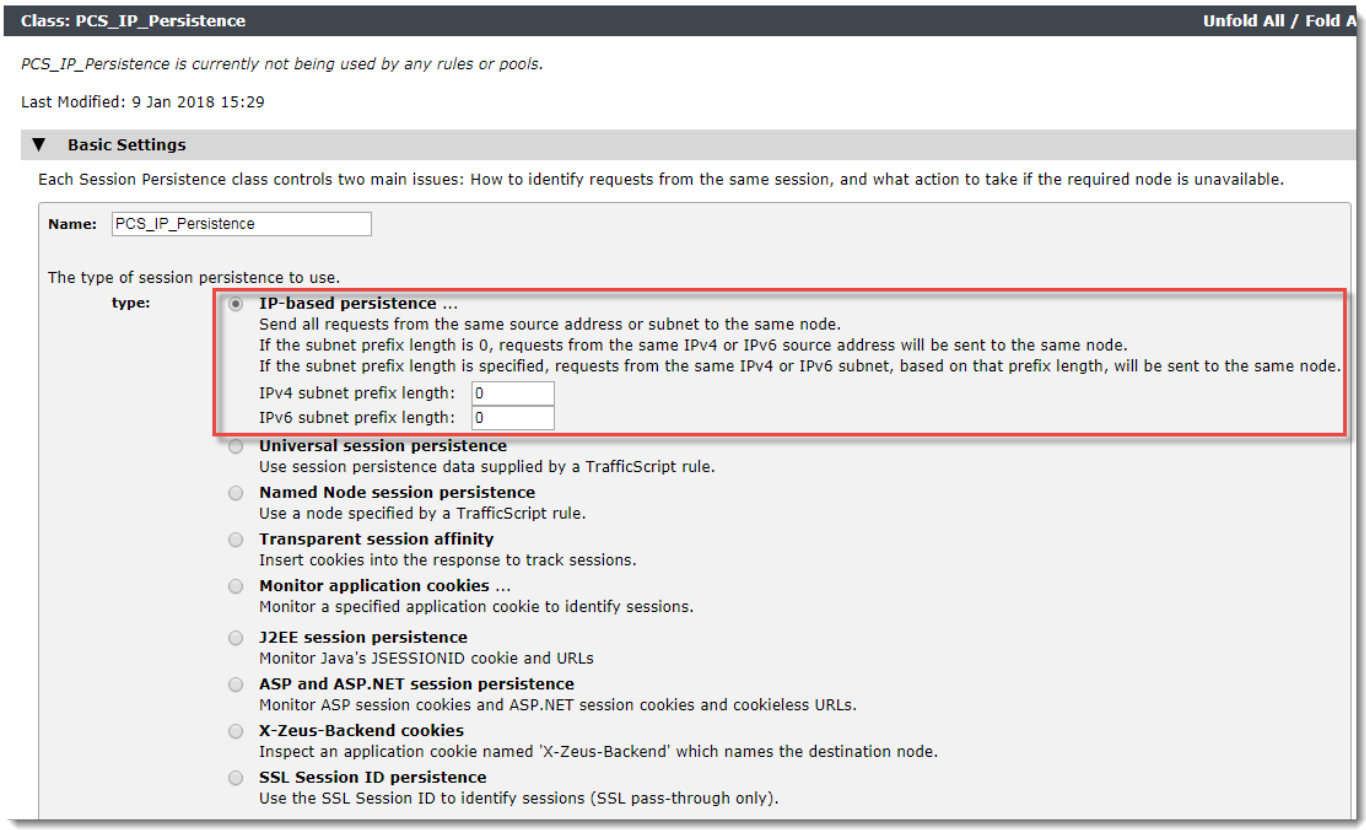
1. Click **Catalogs > Persistence**.
2. In the "Create a new Session Persistence class" section, type a name for the new class and click **Create Class**.

Figure 18 Creating a new Session Persistence Class



3. In the Session Persistence class edit page, ensure that **type** is set to "IP-based persistence". All other settings can remain using their default values.

Figure 19 Setting IP-based Persistence



4. Click **Update** to save any changes.

Creating PCS Pools

To create the configuration described at the beginning of this chapter, create two separate pools both containing the active-active PCS cluster pair as nodes. However, the nodes in each pool use a different port:

- 443 for the secure TCP (SSL) pool

- 4500 for the ESP mode (UDP streaming) pool

To create the required pool configurations, perform the following steps in the Traffic Manager Admin UI. Compete these steps first for TCP and then a second time for ESP:

1. Click **Services > Pools**.
2. In the "Create New Pool" section, enter the details of your new pool. If, for example, your PCS node IP addresses are 192.0.2.250 and 192.0.2.251, create pools with the following values:

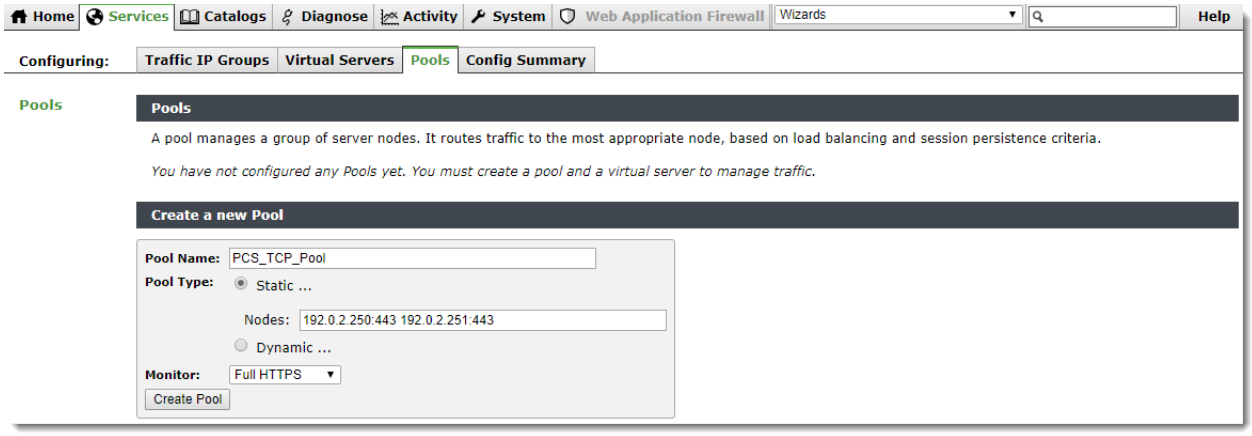
   For the TCP pool:

   - **Pool Name**: Type an identifying name for your pool.
   - **Nodes**: Type "192.0.2.250:443 192.0.2.251:443".
   - **Monitor**: Select "Full HTTPS Monitor".

   For the ESP pool:

   - **Pool Name**: Type an identifying name for your pool.
   - **Nodes**: Type "192.0.2.250:4500 192.0.2.251:4500".
   - **Monitor**: Select "Ping Monitor".

Figure 20 Creating a new pool



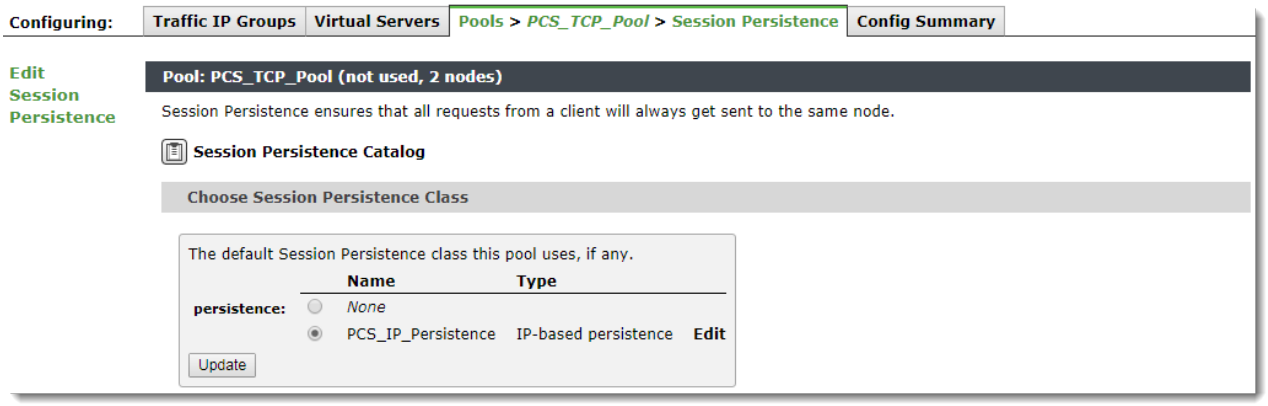
3. To create the new pool, click **Create Pool**.

Additional Required Pool Configuration

After the Traffic Manager creates a new pool, the Edit page is displayed in the Admin UI to facilitate further configuration. For proper load-balancing of PCS instances, the Traffic Manager requires a number of further configuration steps to both pools:

- In the pool edit page, locate the "Session Persistence" section and set **persistence** to the *IP-based Persistence* class created in "Creating an IP-based Session Persistence Class" on page 18.

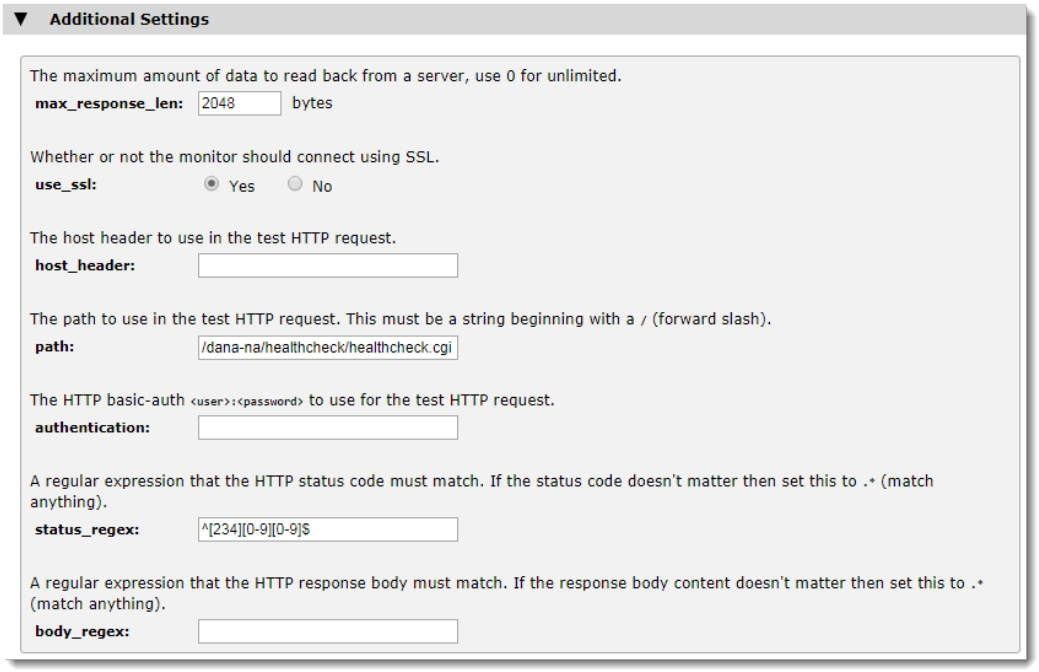
Figure 21 Adding Session Persistence



- For the TCP pool only, click through to the *Full HTTPS* Monitor settings page (through either the link in the TCP pool's Health Monitors section, or by clicking **Catalogs > Monitors > Full HTTPS**) and set **path** to the following value:

  ```
  /dana-na/healthcheck/healthcheck.cgi
  ```

Figure 22 Configuring the Path Used for the HTTP Test



Configuring Virtual Servers in the Traffic Manager

To create the configuration described at the beginning of this chapter, you must create separate virtual servers to handle both TCP and ESP mode traffic. Each virtual server balances traffic across the pool of the same protocol type.

To create the required virtual servers, perform the following steps in the Traffic Manager Admin UI. Complete these steps first for TCP and then a second time for ESP:

1. Click **Services > Virtual Servers**.
2. In the "Create New Virtual Server" section, enter the details of your new virtual server:

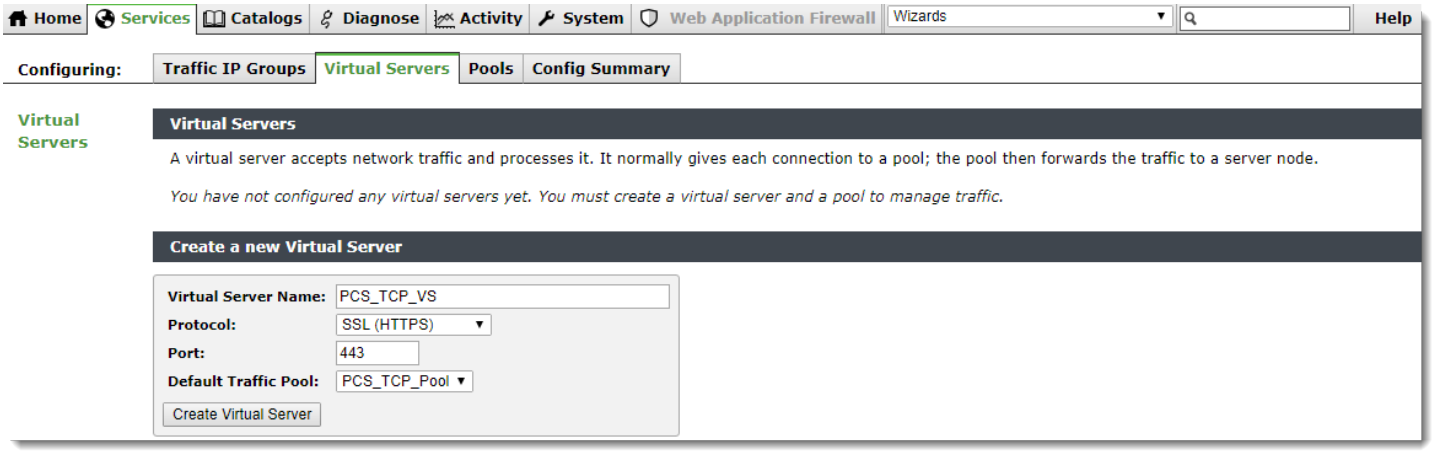
   For the TCP virtual server:

   - **Name**: Type an identifying name for your virtual server.
   - **Protocol**: Select "SSL (HTTPS)".
   - **Port**: Use the value "443".
   - **Default Traffic Pool**: Select your previously created TCP pool.

   For the ESP mode virtual server:

   - **Name**: Type an identifying name for your virtual server.
   - **Protocol**: Select "UDP - Streaming".
   - **Port**: Use the value "4500".
   - **Default Traffic Pool**: Select your previously created ESP mode pool.

Figure 23 Creating a new Virtual Server



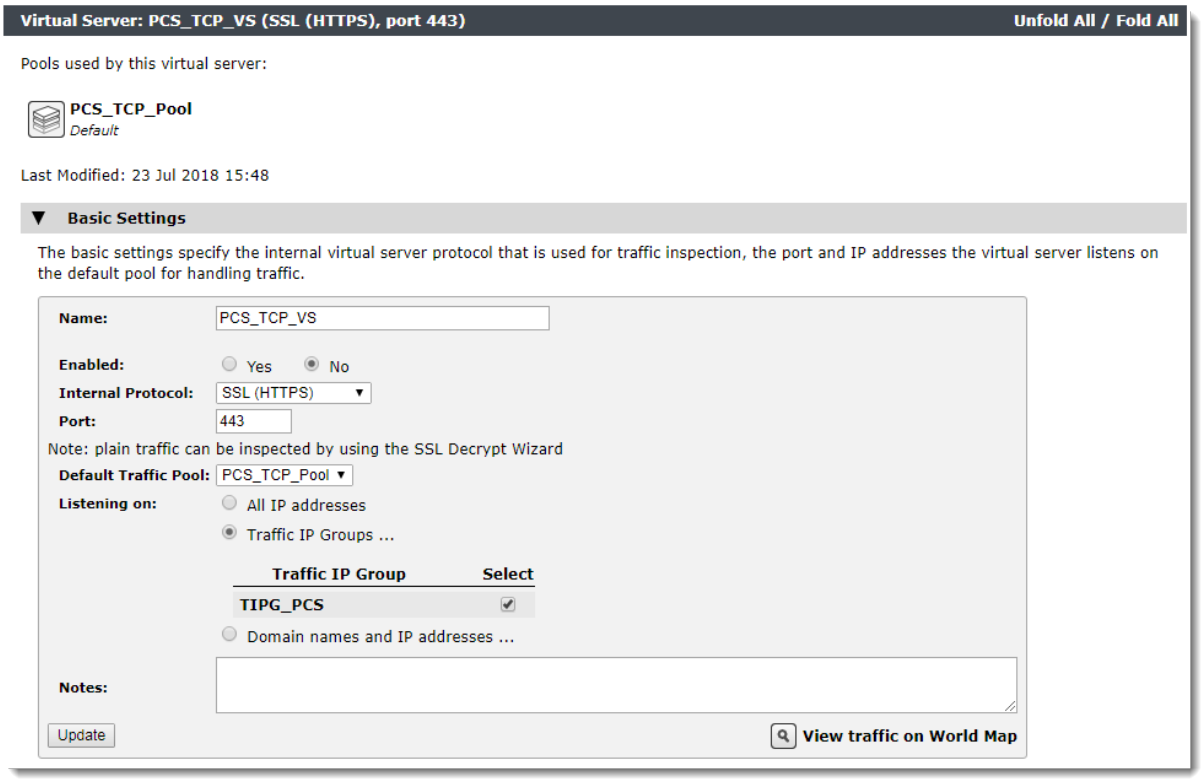
3. To create a virtual server based on these settings, click **Create Virtual Server**.

Additional Required Virtual Server Configuration

After the Traffic Manager creates a new virtual server, the Edit page is displayed in the Admin UI to facilitate further configuration. For proper load-balancing of PCS instances, the Traffic Manager requires a number of further configuration steps to both virtual servers:

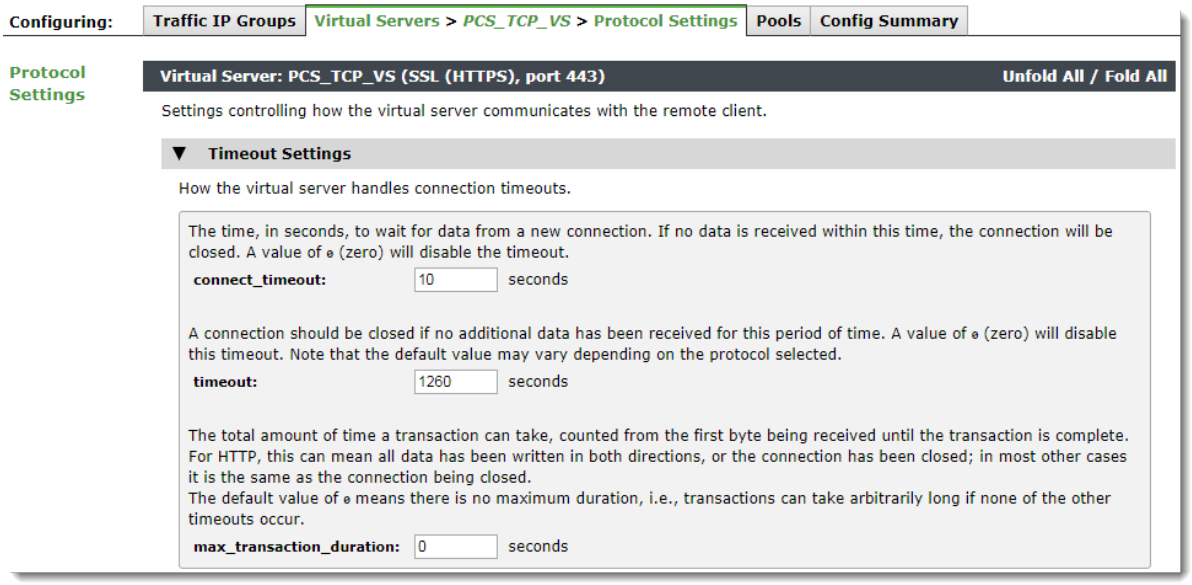
- Set **Listening on** to the name of the Traffic IP Group created in "Creating a Traffic IP Group" on page 17.

Figure 24 Associating a Traffic IP Group with Your Virtual Server



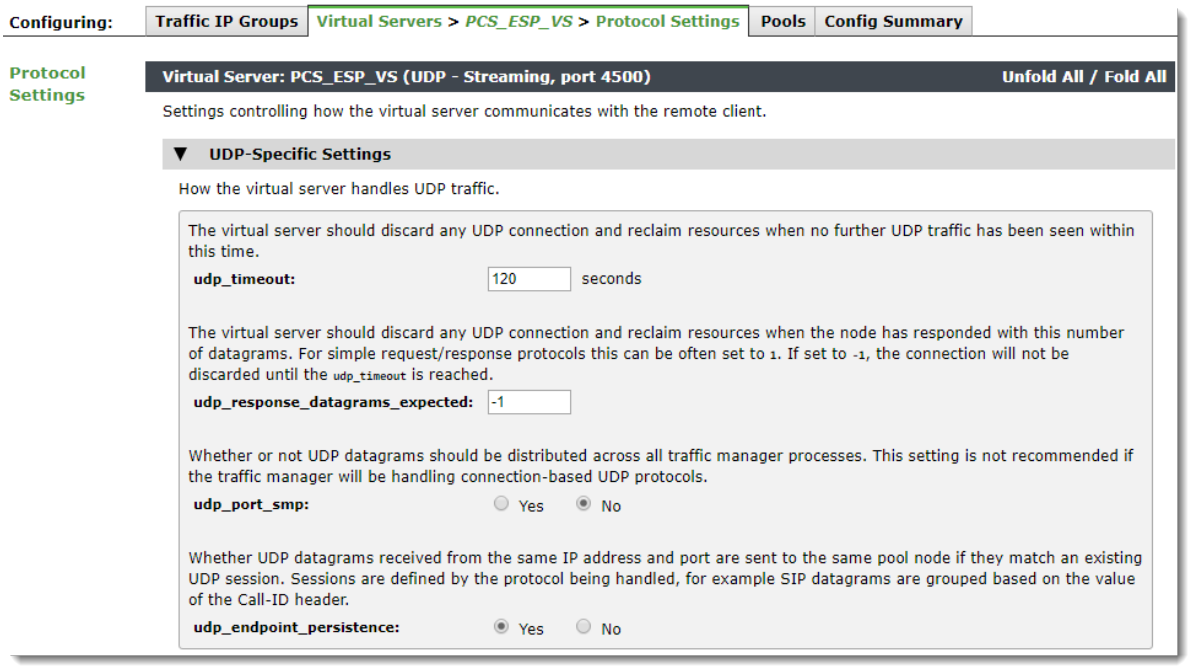
- For the TCP virtual server, in the virtual server edit page, locate the “Protocol Settings” section. Set **timeout** to “1260”.

Figure 25 Setting the HTTP Connection Timeout



- For the ESP mode virtual server, in the virtual server edit page, locate the “Protocol Settings” section. Set **udp_timeout** to “120”.

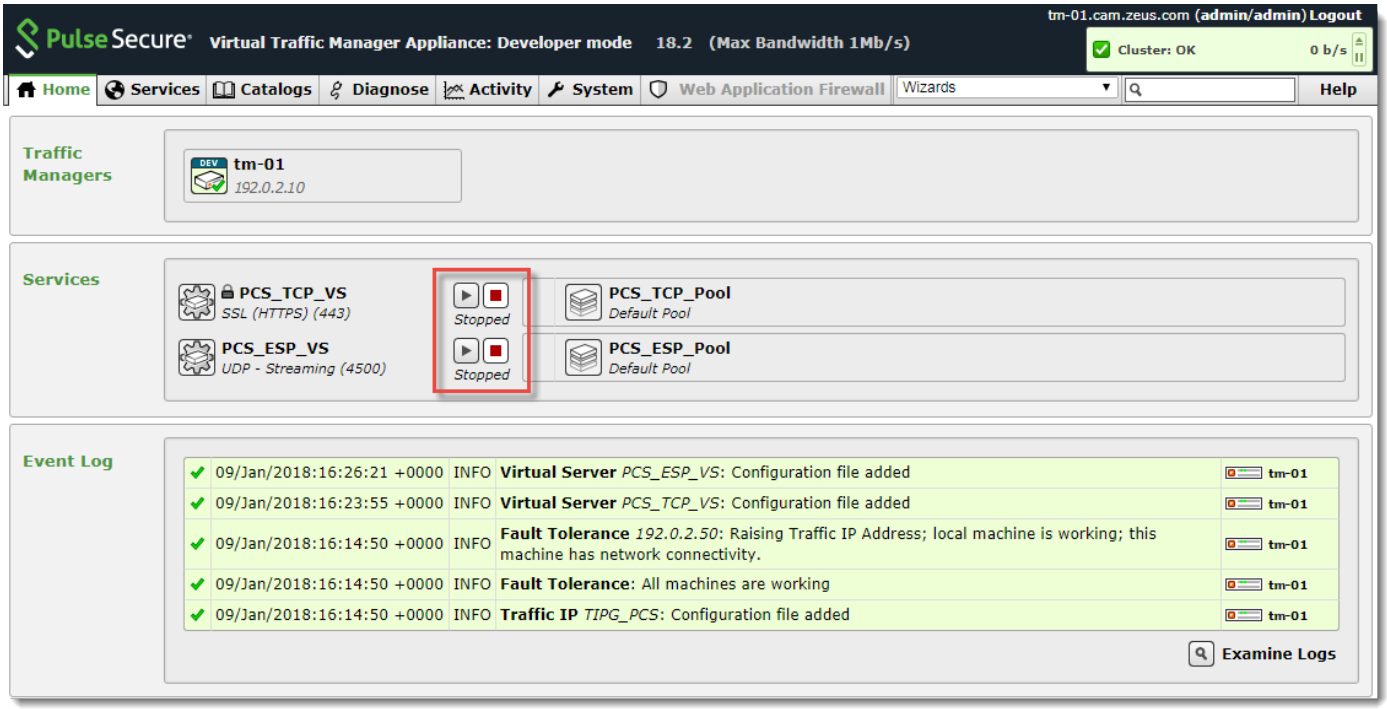
Figure 26 Setting the UDP Timeout



Starting your Services

Your services are created in a disabled state. To allow them to receive traffic, you must first enable each virtual server from either the Home Page or from the individual virtual server edit pages.

Figure 27 Starting Your Services Through the Home Page



To start or stop a virtual server from the Home Page, click the corresponding *Play* or *Stop* icon. The Event Log displays the outcome of each action, providing feedback on any communication or service disruption issues that arise.

Optional: Configuring IP Transparency

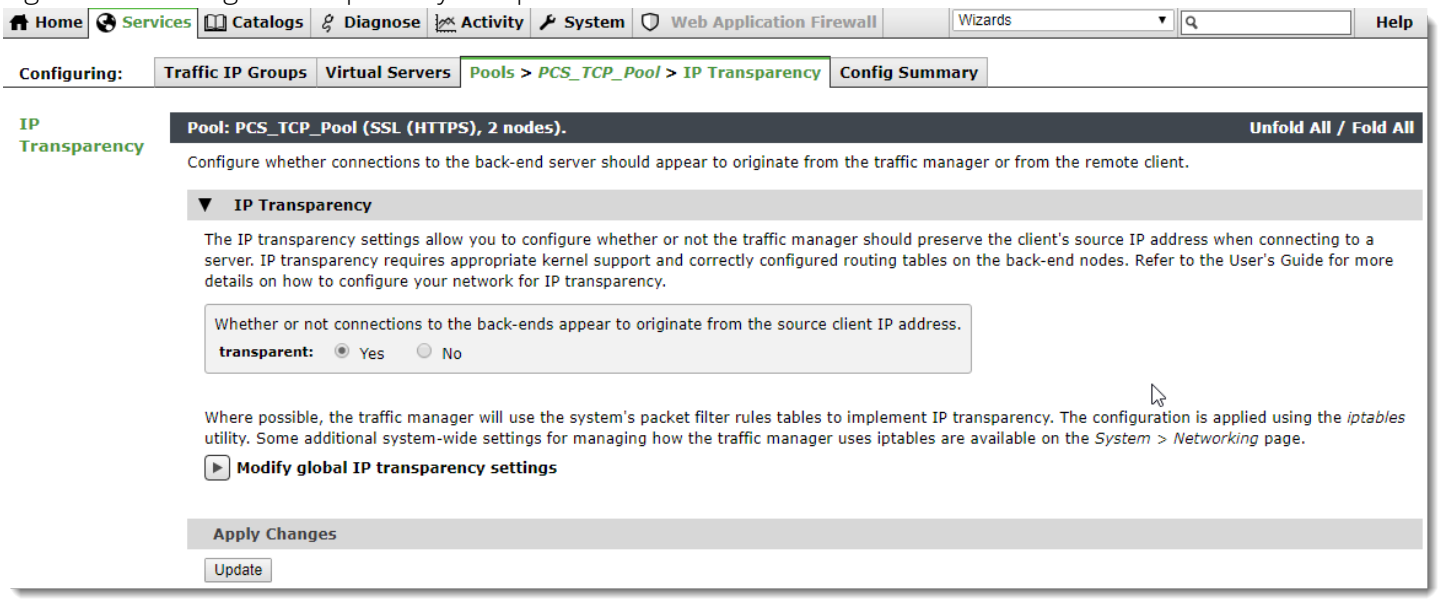
The manual configuration steps described in this guide provide basic load-balancing services for your PCS cluster. The Traffic Manager listens for incoming connections and balances them across your PCS nodes. A PCS node sees the incoming traffic as having originated from the Traffic Manager's back-end IP address, and so sends a response back to the same address. The Traffic Manager then passes this response back to the client.

In some circumstances, you might want to propagate the client IP address through to the PCS node, such that PCS observes the connection as having originated from the client's own IP address rather than the IP address of the Traffic Manager. For this scenario, configure your Traffic Manager's PCS pools with *IP transparency*.

To enable transparency for a pool, perform the following steps:

1. Login to the Traffic Manager Admin UI
2. Click **Services > Pools**.
3. Click the name of the pool you want to modify.
4. In the pool edit page, click **IP Transparency**.
5. Set **transparent** to "Yes".
6. Click **Update** to apply the change.

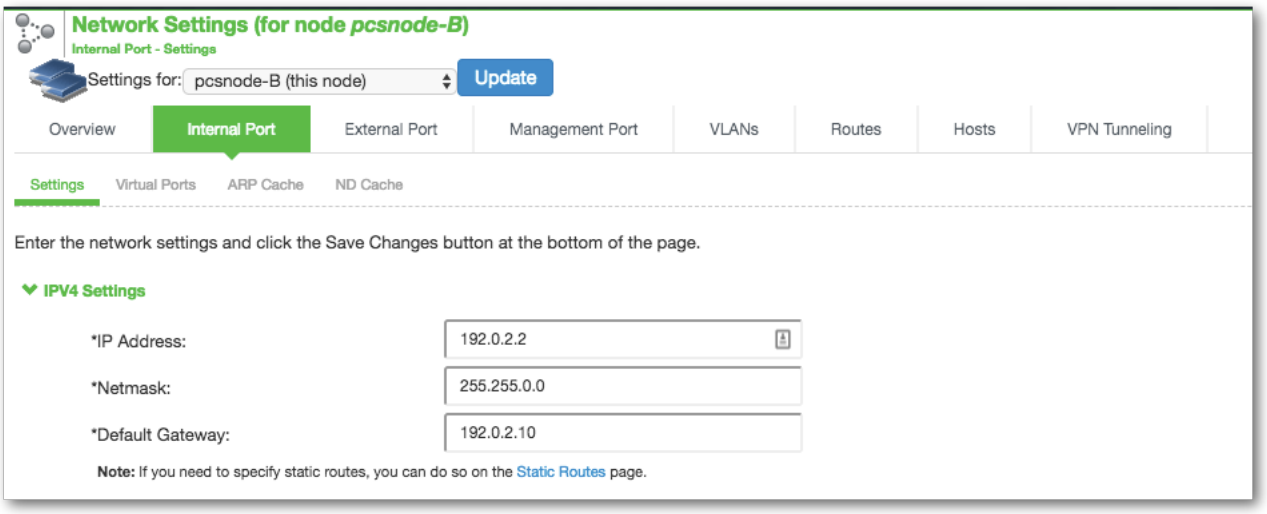
Figure 28 Adding IP transparency to a pool



7. Repeat the procedure as necessary to ensure transparency is enabled for both the SSL pool and UDP streaming pool.

With transparency enabled, PCS observes a request as having originated from a remote client rather than the Traffic Manager and consequently addresses its responses back to the same client IP address. However, for transparency to operate correctly, each PCS instance must route its responses back through the Traffic Manager that sent the request. To achieve this, configure your PCS instances to use the Traffic Manager as the default gateway.

Figure 29 Setting the PCS default IPv4 gateway



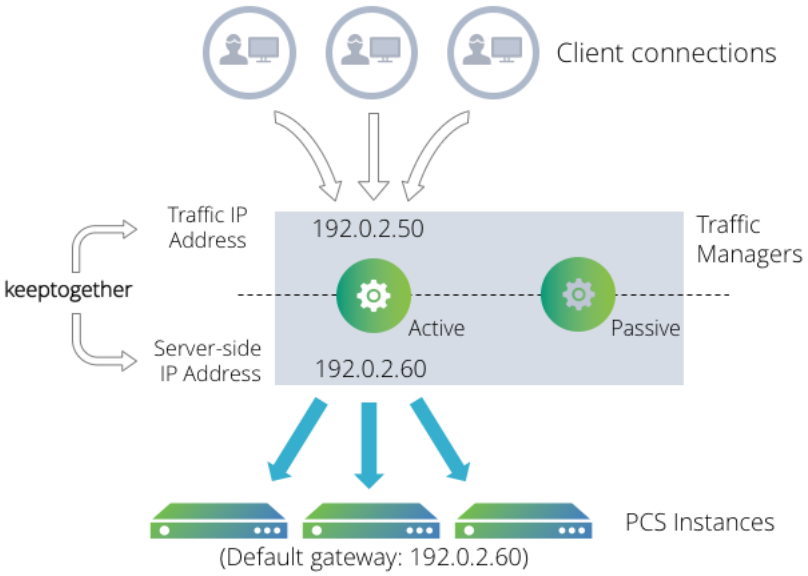
For singular Traffic Manager instance deployments, this arrangement is straightforward. All PCS instances receive requests from the same Traffic Manager, and route responses back to the same gateway address. For Traffic Manager clusters, requests could be received from any Traffic Manager instance in the cluster; which in turn requires more careful gateway routing configuration.

Configuring Transparency with a Traffic Manager Cluster

Using IP transparency with a cluster of Traffic Managers introduces additional complexity because each PCS instance is configured to route traffic to a single gateway IP address. However, any of the Traffic Managers in the cluster can send transparent connections to a PCS instance, and each PCS must route the response back to the Traffic Manager that originated the connection.

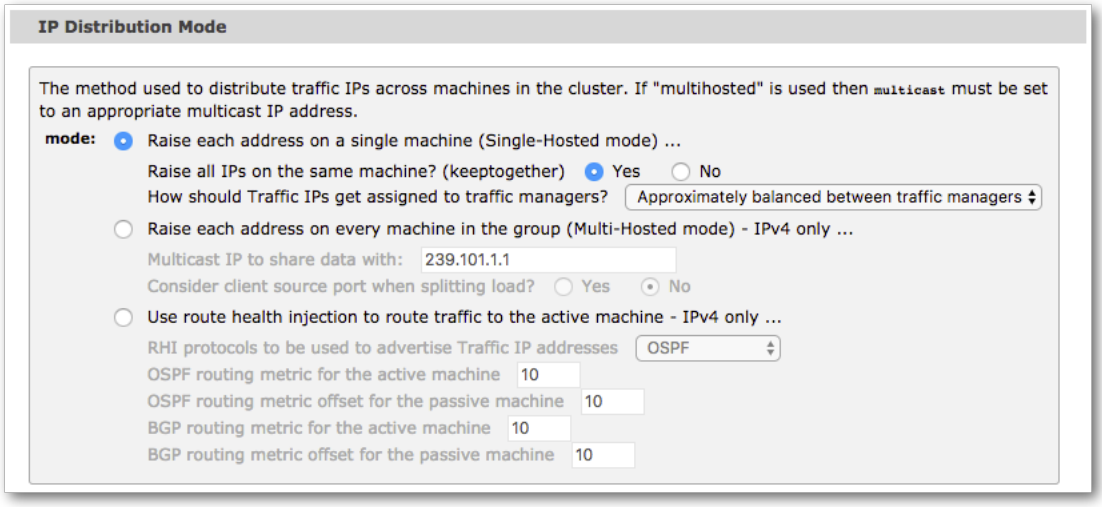
To address this problem, use a traffic IP group in your Traffic Manager cluster containing two IP addresses; the front-end IP address for incoming client traffic, and a back-end IP address that resides on the server side network. To ensure response traffic is routed to the originating Traffic Manager, use the **keeptogether** option.

Figure 30 Configuring a Traffic IP group to bind together the Traffic IP address and server-side IP address



The scenario described earlier in this guide uses a traffic IP group to provide a fault-tolerant service IP address. Modify this traffic IP group by adding the back-end server side IP address. Then, ensure both IP addresses are raised on the same Traffic Manager by setting the **keeptogether** option to yes.

Figure 31 Enabling "keeptogether" in the traffic IP group



Finally, set the default gateway on each PCS instance to the server side IP address used in the traffic IP group. For more details, see Figure 29 on page 26.

To learn more about Traffic IP addresses and groups, see "Creating a Traffic IP Group" on page 17.

To learn more about traffic routing with IP transparency, see the "Network Layouts" chapter of the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Optional: Weighted Load Balancing with Service Discovery

Note: This section is optional, and applicable only to deployments consisting of Pulse Secure Virtual Traffic Manager 19.3 and later, and Pulse Connect Secure 9.1R3 and later.

The Traffic Manager can use a feature called Service Discovery to query the number of free license seats on each PCS instance in your deployment. The Traffic Manager can then use this information with weighted load balancing to avoid over-provisioning a single PCS instance.

The Traffic Manager uses the PCS *healthcheck* API to discover the number of free license seats, and in turn to bias new connections to devices that report they have a greater license capacity.

To use this feature, first configure PCS to accept healthcheck requests from your Traffic Manager cluster. Then, configure the Traffic Manager to use the API to send requests to your PCS instances.

Configuring PCS to Accept Healthcheck Requests

Your PCS instances must be configured with the list of devices that should be allowed to make healthcheck requests. To configure PCS to accept healthcheck requests from all Traffic Managers in your cluster, login to the PCS Admin UI and click **System > Configuration > Health Check Options**. Use this page to add each of your Traffic Manager's back-end IP address to the list of devices authorized to perform healthcheck requests. Repeat this step on all PCS instances.

Configuring the Traffic Manager to use the Healthcheck API

To instruct your Traffic Managers to use the healthcheck API, reconfigure your PCS pools in the Traffic Manager Admin UI to use the built-in PCS Service Discovery plug-in.

Prior to configuring your pools, you can test healthcheck API connectivity from the Service Discovery catalog page. This can help validate that PCS has been correctly configured, that the plug-in arguments are syntactically correct, and that your PCS instances are of the correct software version to provide license data. To test the plug-in, login to the Traffic Manager Admin UI and click **Catalogs > Service Discovery**. Locate the *BuiltIn-PCS_PPS* plug-in and use the "Test plugin" section to send a test argument string to the plug-in. For the correct argument syntax, see the entry for "service_discovery!plugin_args" in the following table.

After you have successfully tested API connectivity, edit your PCS pool configuration and select the Service Discovery sub-section (click **Services > Pools > Edit > Service Discovery**). From this page, complete the following required configuration items:

Configuration Item	Setting
service_discovery!enabled	Set to "Yes"
service_discovery!plugin	Select "builtin-PCS_PPS"

Configuration Item	Setting

service_discovery!plugin_args	For the HTTPS pool, use the following argument:
	`--nodes="192.0.2.0:443 192.0.2.1:443" --info`
	
	For the ESP pool, use the following argument:
	`--nodes="192.0.2.0:4500 192.0.2.1:4500" --info`
	
	For the `--nodes` argument, substitute in a space or comma separated list of your PCS node IP addresses, as also specified during the "Load-balance Pulse Connect Secure" wizard (see Figure 14 on page 14).
	The `--info` argument places INFO messages in the Traffic Manager Event Log whenever a change is detected in the relative node weights (used by the load-balancing algorithm). If such log message are not required, you can safely omit this argument.
	Note: For the ESP pool, make sure the port number you use matches that specified during the "Load-balance Pulse Connect Secure" wizard (see Figure 12 on page 13).
	To test an argument string without reconfiguring your pools, use the "Test Plugin" section in the *Builtin-PCS_PPS* Service Discovery catalog page.

To save your changes, click **Update**. Note that in the pool edit page, the node list is no longer configurable.

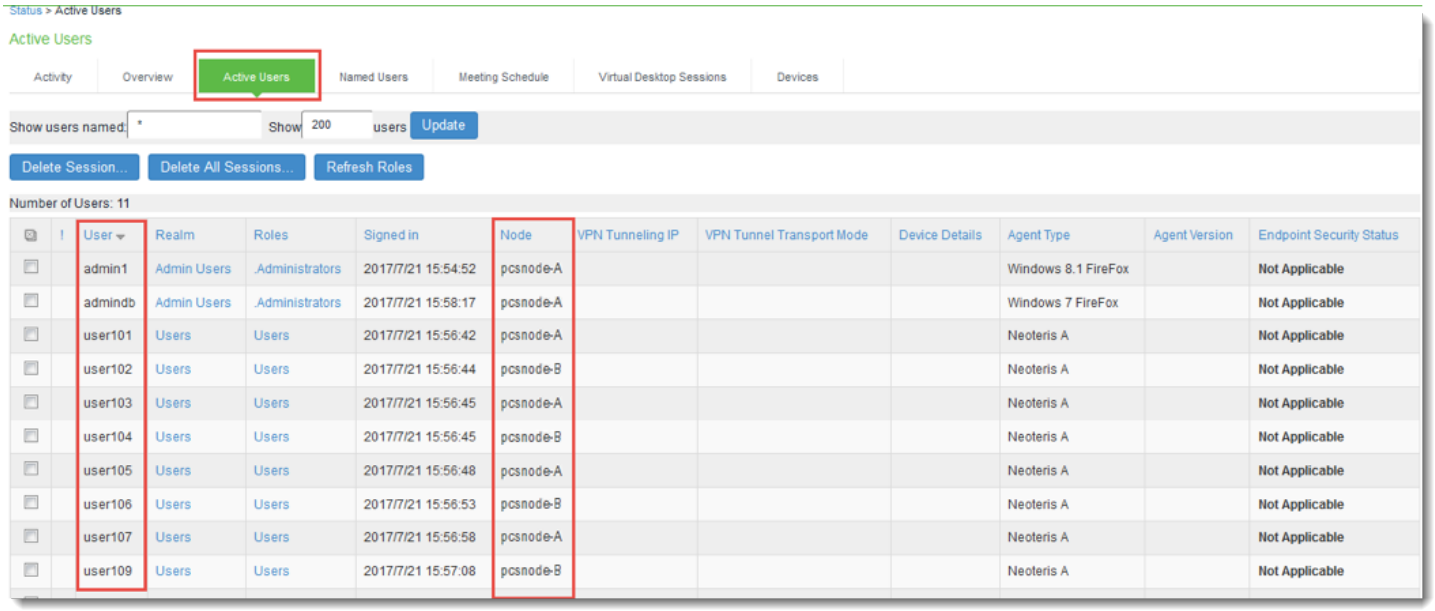
Next, select a "Weighted" load-balancing algorithm (click **Services > Pools > Edit > Load Balancing**). You must complete this process for both PCS pools in your Traffic Manager configuration.

To learn more about Service Discovery, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Verifying Operation

To view the traffic for active users currently connected to your Pulse Connect Secure (PCS) cluster pair, login to the PCS Admin UI and click **System > Status > Active Users**. This page displays a list of active users and the PCS node to which they are connected.

Figure 32 Active users.



!	User	Realm	Roles	Signed in	Node	VPN Tunneling IP	VPN Tunnel Transport Mode	Device Details	Agent Type	Agent Version	Endpoint Security Status
	admin1	Admin Users	Administrators	2017/7/21 15:54:52	pcsnode-A				Windows 8.1 FireFox		Not Applicable
	admindb	Admin Users	Administrators	2017/7/21 15:58:17	pcsnode-A				Windows 7 FireFox		Not Applicable
	user101	Users	Users	2017/7/21 15:56:42	pcsnode-A				Neoteris A		Not Applicable
	user102	Users	Users	2017/7/21 15:56:44	pcsnode-B				Neoteris A		Not Applicable
	user103	Users	Users	2017/7/21 15:56:45	pcsnode-A				Neoteris A		Not Applicable
	user104	Users	Users	2017/7/21 15:56:45	pcsnode-B				Neoteris A		Not Applicable
	user105	Users	Users	2017/7/21 15:56:48	pcsnode-A				Neoteris A		Not Applicable
	user106	Users	Users	2017/7/21 15:56:53	pcsnode-B				Neoteris A		Not Applicable
	user107	Users	Users	2017/7/21 15:56:58	pcsnode-A				Neoteris A		Not Applicable
	user109	Users	Users	2017/7/21 15:57:08	pcsnode-B				Neoteris A		Not Applicable

To view the IP address for each user, click **System > Log/Monitoring > User Access > Log**.

Figure 33 User Access Log