



Optimal Gateway Selection for Pulse Connect Secure with Pulse Secure Virtual Traffic Manager

Deployment Guide

Published

14 December, 2017

Document Version

1.0

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

www.pulsesecure.net

© 2017 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Optimal Gateway Selection for 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.....	3
PURPOSE OF THIS GUIDE.....	3
PREREQUISITES.....	3
THE CHALLENGE.....	3
THE SOLUTION.....	4
CONFIGURATION SUMMARY.....	5
CONFIGURING THE TRAFFIC MANAGER AS A DNS SERVER.....	7
CREATING A GSLB SERVICE.....	11
SETTING UP YOUR PCS GATEWAYS AS GLB LOCATIONS IN THE TRAFFIC MANAGER.....	11
CREATING GLB LOCATION MONITORS.....	12
CREATING A GLB SERVICE.....	14
ADDING GSLB FUNCTIONALITY TO YOUR TRAFFIC MANAGER DNS SERVICE.....	17

Introduction

Purpose of this Guide

This guide describes how to configure Pulse Secure Virtual Traffic Manager (the Traffic Manager) to provide optimal gateway selection and dynamic failover when deploying multiple geographically-located Pulse Connect Secure (PCS) clusters.

Prerequisites

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

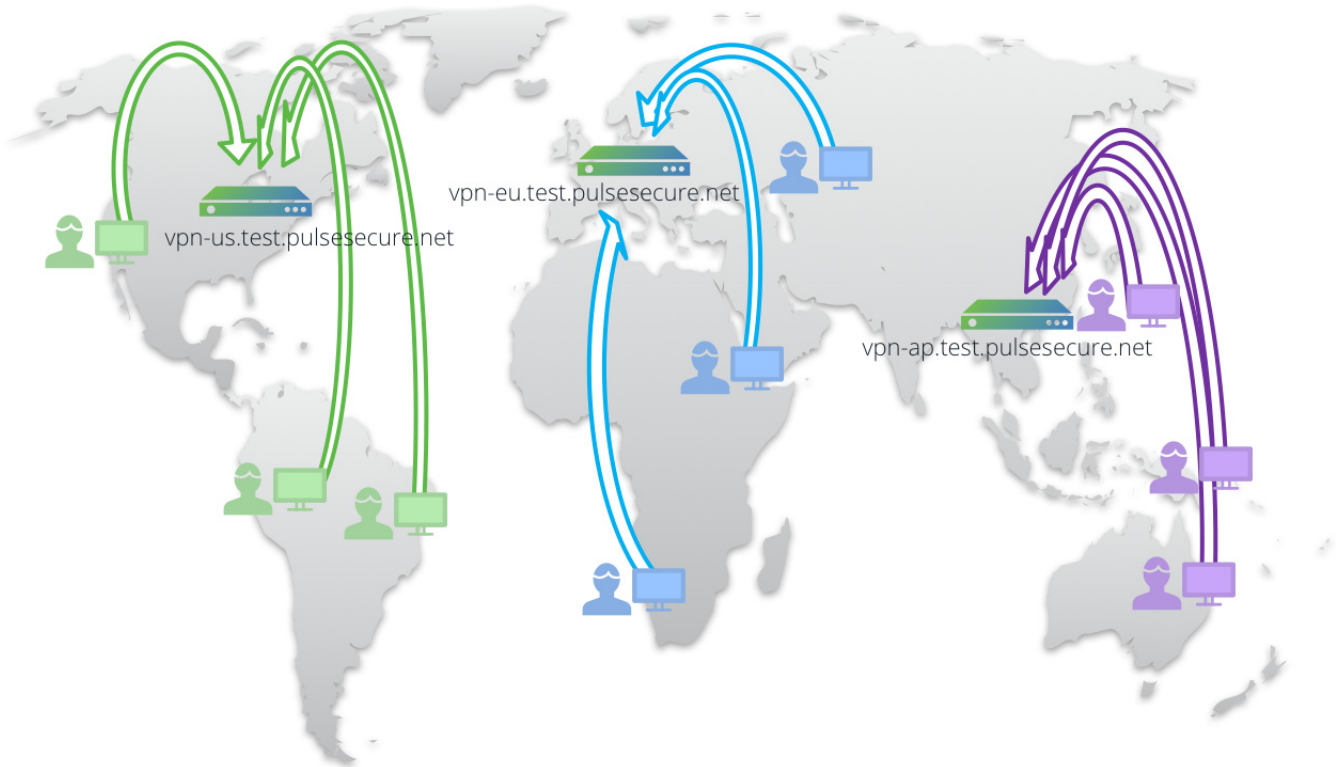
This guide does not cover the initial installation tasks associated with setting up PCS or the Traffic Manager. The steps referred to in this guide assume you have a fully working and licensed set of PCS and Traffic Manager instances.

This guide also assumes you are familiar with the Domain Name System (DNS).

The Challenge

An organization can deploy multiple instances of Pulse Connect Secure (PCS) across a series of global data center locations to provide secure remote access facilities to users local to that region. Each location might contain a single PCS device, or possibly a cluster of PCS devices to ensure service availability in the event of a single device failure. However, in the event of regional disruption, total service loss is possible.

FIGURE 1 Connecting to geographically-distributed VPN endpoints



Furthermore, users must manually determine the optimal PCS gateway for their needs at any given geographic location. Configuration and URL settings for all locations must be maintained across all users and all devices.

If complete failure occurs at any one location, user or admin intervention is required to force failover to an alternate PCS gateway in another location.

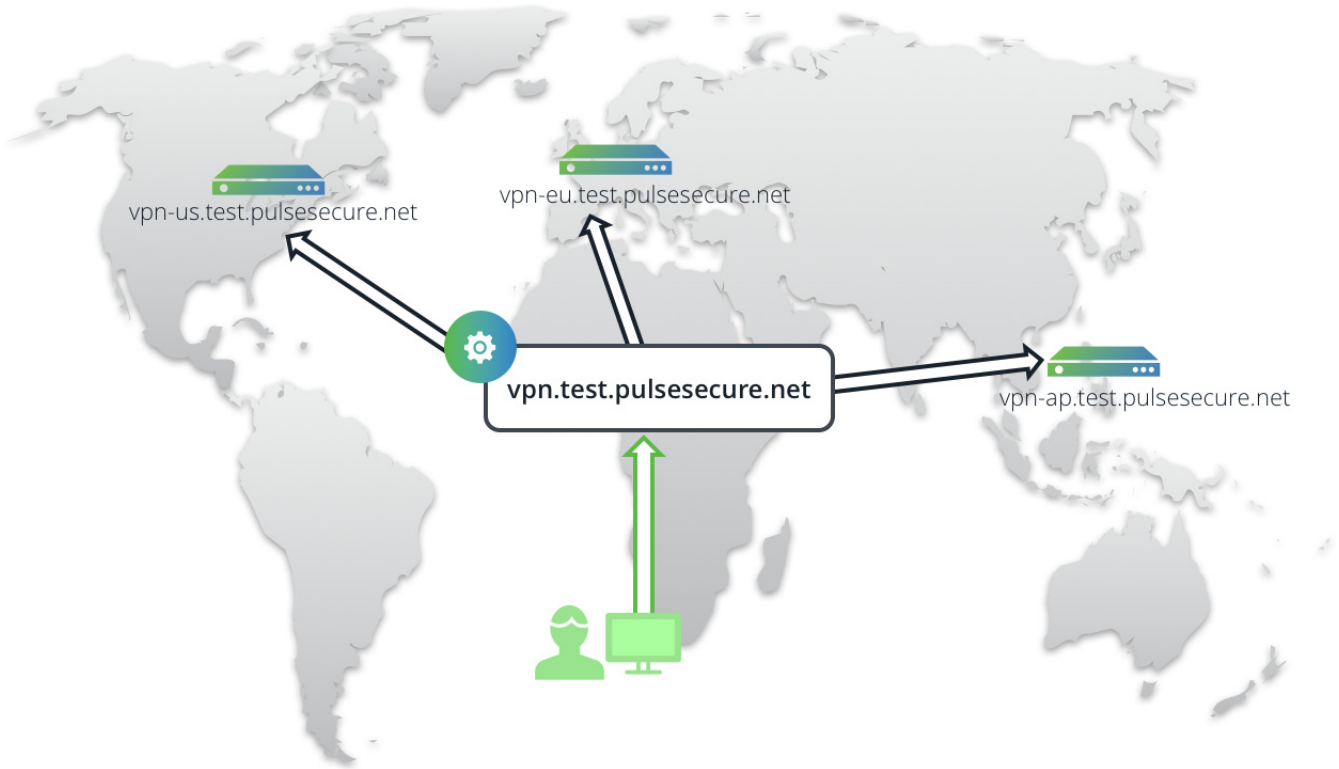
The Solution

Enterprise-wide High Availability is achieved through the implementation of DNS-based Global Server Load Balancing (GSLB), whereby users connect to a single unified organization-wide endpoint URL, with the GSLB service providing optimum gateway selection and dynamic failover based on a series of observed criteria:

- The geographic location of the user relative to the nearest available PCS gateway
- The current availability of the selected PCS gateway
- The measured load on the selected PCS gateway

To provide the GSLB function, deploy Pulse Secure Virtual Traffic Manager as an authoritative DNS server (or alternatively as a proxy for a separate back-end DNS service).

FIGURE 2 Connecting to a single unified organization-wide endpoint



When the Traffic Manager receives a DNS request from a client for the unified endpoint URL, the Traffic Manager adds location-awareness to the DNS lookup, such that the result of the lookup becomes dependent upon its source. It determines and modifies the response, based on configurable metrics (such as geographic proximity and load), before sending the response back to the client.

The Traffic Manager continually monitors the health of all PCS endpoint locations, and automatically redirects users to a working location in the event of service failure.

Making changes to your PCS infrastructure later, such as replacing one location with another, requires an update only to your Traffic Manager configuration. All users continue to use the unified endpoint URL, with no client configuration updates required.

Configuration Summary

The procedure outlined here assumes the organizational domain "test.pulsesecure.net", containing three geographically-separate PCS deployments with the following public IP addresses:

Hostname	IP Address
vpn-us.test.pulsesecure.net	192.0.2.1
vpn-eu.test.pulsesecure.net	192.0.2.2
vpn-ap.test.pulsesecure.net	192.0.2.3

The intention is to replace all local PCS endpoints in your client configuration with a single unified endpoint: “vpn.test.pulsesecure.net”.

For the purposes of this guide, we assume that each local endpoint exposes a VPN service at a single public IP address, and the endpoint health status can be determined by monitoring a URL at the same IP address. The actual network topology at each endpoint is out of scope.

The following instructions assume you have previously deployed your PCS instances, and have subsequently deployed two or more Traffic Managers in a cluster ready for configuration.

To configure your Traffic Manager for GSLB, perform the following steps:

1. Configure the Traffic Manager as a DNS server to handle incoming DNS requests. Add a DNS zone file with hostname mappings for each of your PCS location IP addresses, and with the hostname mapping for your new unified endpoint URL.
2. Create a GSLB service in the Traffic Manager, using the following steps:
 - a. Add each of your PCS endpoints as Global Load Balancing (GLB) Locations, and create new service health monitors for each location.
 - b. Create a new GLB Service based on your pre-defined GLB Locations.
 - c. Add your GLB Service to the DNS virtual server.
 - d. Set your end client configuration to connect to the new endpoint URL.

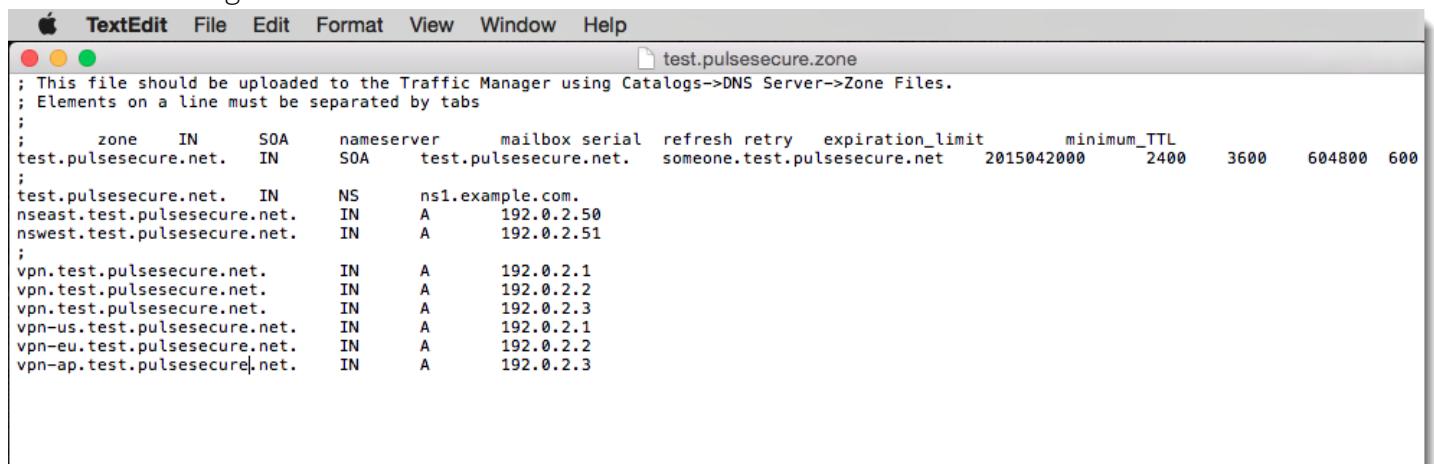
Configuring the Traffic Manager as a DNS server

To configure the Traffic Manager as a DNS server, perform the following steps:

1. Using a text editor, create a DNS zone file and add to it the hostname to IP address mappings for each of your PCS gateways. Then, add a mapping for the new unified gateway URL to all the individual PCS gateway IP addresses. The following is an example of the relevant entries to be added to a zone file:

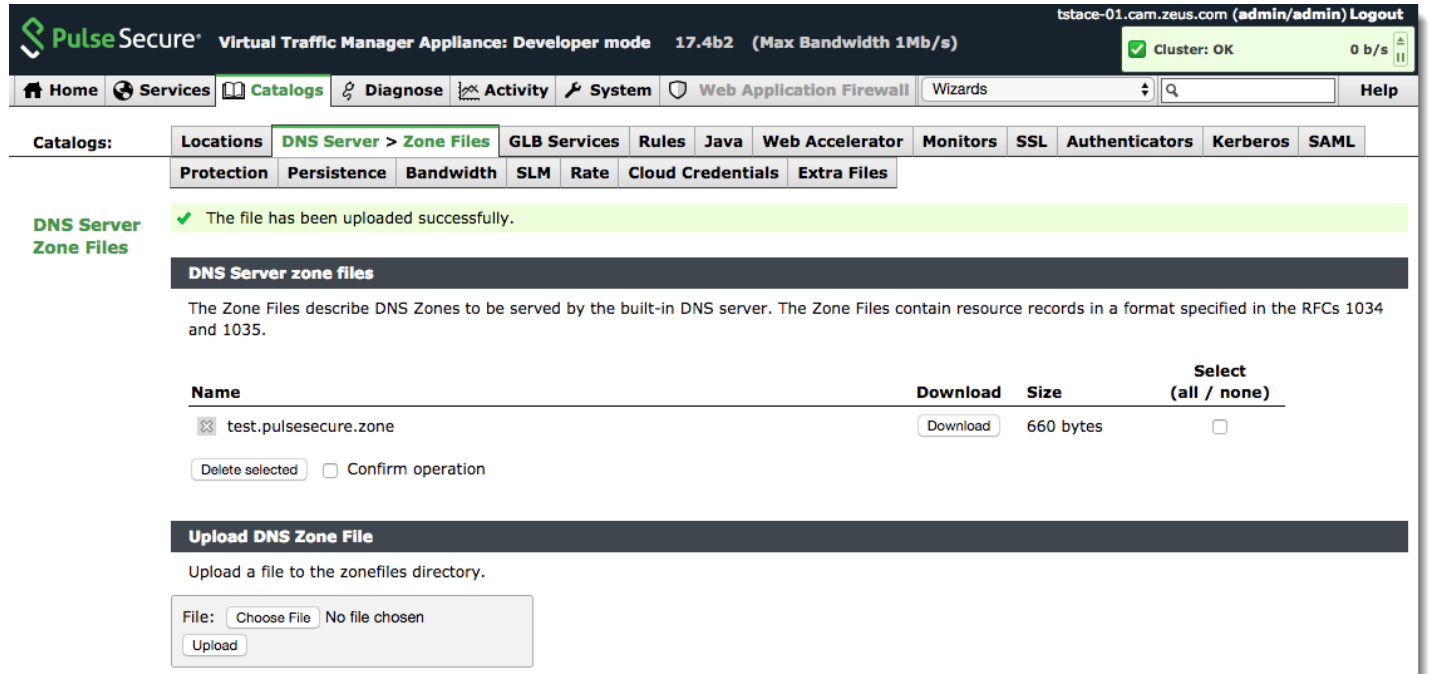
```
vpn.test.pulsesecure.net.      IN      A       192.0.2.1
vpn.test.pulsesecure.net.      IN      A       192.0.2.2
vpn.test.pulsesecure.net.      IN      A       192.0.2.3
vpn-us.test.pulsesecure.net.   IN      A       192.0.2.1
vpn-eu.test.pulsesecure.net.   IN      A       192.0.2.2
vpn-ap.test.pulsesecure.net.   IN      A       192.0.2.3
```

FIGURE 3 Editing a DNS zone file



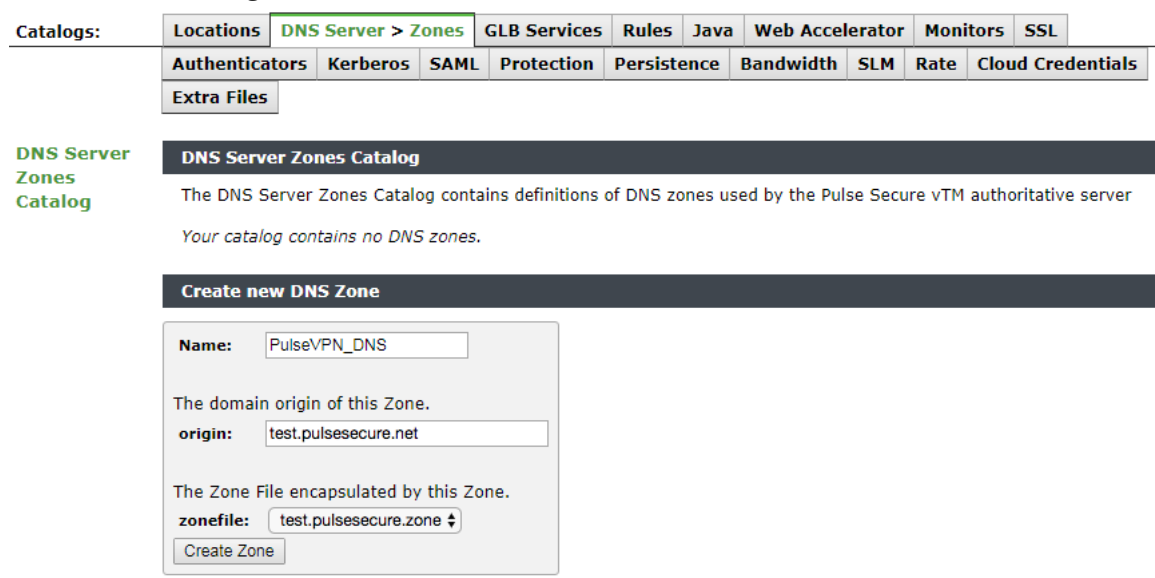
2. To upload the zone file to the Traffic Manager, login to the Admin UI and click **Catalogs > DNS Server > Zone Files Catalog**. Follow the instructions to upload your file.

FIGURE 4 Uploading a DNS zone file



- To use this zone file in a Traffic Manager DNS service, associate the zone file with a DNS Zone. Click **Catalogs > DNS Server > Zone Catalog**. Enter the details of your new zone in the "Create new DNS Zone" section:
 - **Name:** The identifying name for your zone
 - **Origin:** The domain origin for your zone. In this example, use "test.pulsesecure.net"
 - **Zonefile:** Select the zonefile uploaded in the previous step

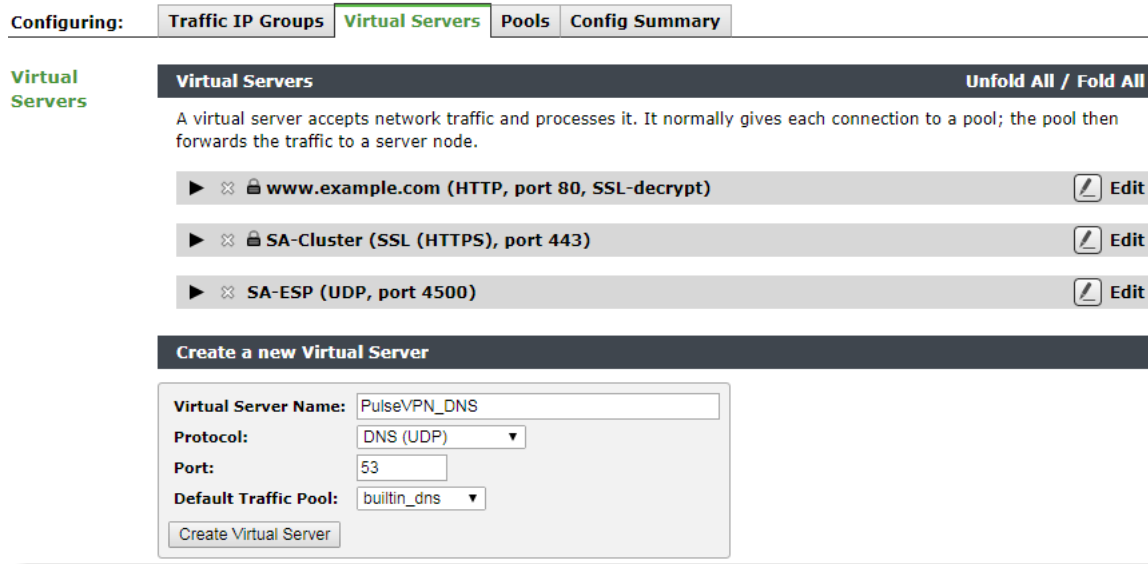
FIGURE 5 Creating a DNS Zone



- To create the DNS zone, click **Create Zone**.

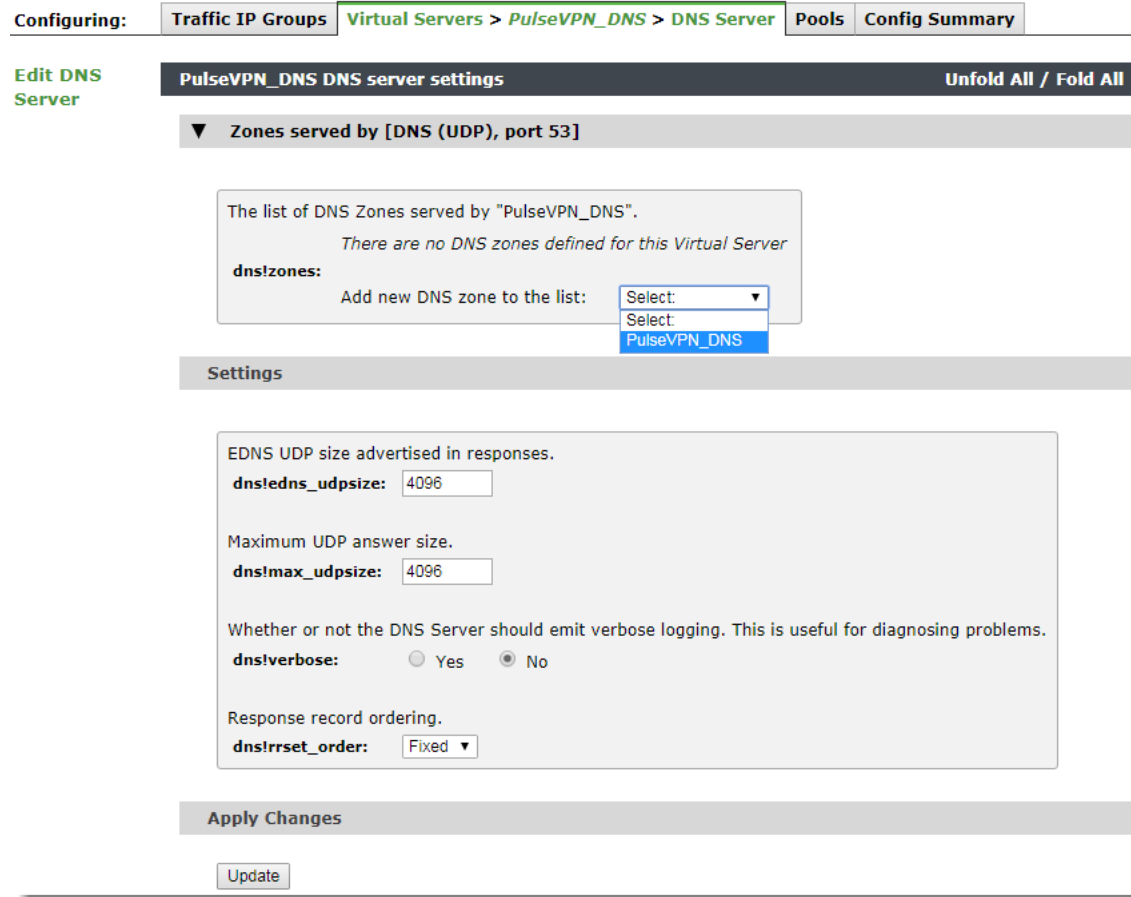
5. To create a DNS service running on the Traffic Manager, click **Services > Virtual Servers**.
6. Create a new virtual server with the following settings:
 - **Name:** The identifying name for your virtual server.
 - **Protocol:** Select "DNS (UDP)".
 - **Port:** Type "53".
 - **Default Traffic Pool:** Select "builtin_dns".

FIGURE 6 Creating a DNS virtual server



7. To create a virtual server based on these settings, click **Create Virtual Server**.
8. In the virtual server edit page, click **DNS Server**.
9. Set **dns!zones** to the DNS Zone created earlier, then click **Update**.

FIGURE 7 Adding a DNS Zone to a virtual server



10. In the virtual server edit page, enable your virtual server by setting **Enabled** to "Yes". Click **Update** to save your changes.

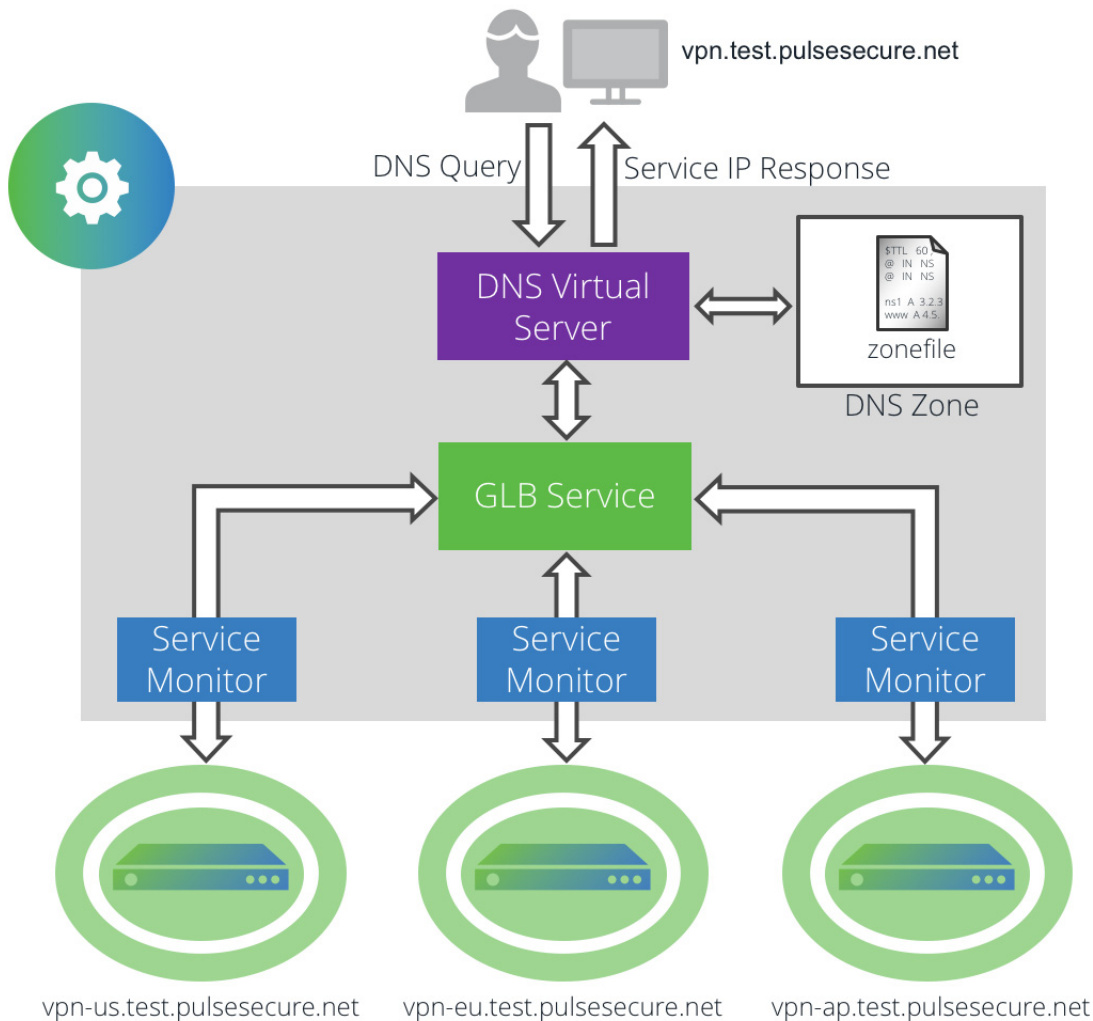
By setting your client networking configuration to use the Traffic Manager's public IP address as a name server, the Traffic Manager is now able to respond to DNS requests for the individual PCS gateway URLs (for example, "vpn-eu.test.pulsesecure.net"), and also for the unified gateway URL ("vpn.test.pulsesecure.net").

In the case of the latter, a request should return all three local PCS IP addresses as stated in the zone file.

Creating a GSLB Service

The Traffic Manager implements GSLB techniques as the Global Load Balancer (GLB) feature. The GLB feature consists of a number of components, that together enable the Traffic Manager to add location-awareness to DNS lookups performed by end-users. The sections that follow describe how to configure each of the components separately, and then how to combine them into a fully-functioning GSLB service.

FIGURE 8 Structure of a GSLB service in the Traffic Manager



Setting up your PCS Gateways as GLB Locations in the Traffic Manager

A Traffic Manager Global Load Balancing (GLB) Location is defined by its geographic position in the world. A GLB Location is used by a GLB Service to determine where DNS responses should direct clients.

To define your PCS endpoints as GLB Locations, perform the following steps:

1. Login to the Traffic Manager Admin UI.
2. Click **Catalogs > Locations Catalog**.
3. In the "Create New GLB Location" section, type a suitable identifying name for the new PCS endpoint location and click **Add Location**.
4. In the location settings page, set **Position** to the geographic location of your PCS endpoint. Select either a country from the drop-down list, a set of latitude and longitude coordinates, or set the location manually using the drag-and-drop map.

FIGURE 9 Choosing a location using the world map

The screenshot shows the 'Settings' page for a location named 'Loc-EU'. The 'Position' section has four radio button options: 'No position', 'Select a country ...', 'Specify latitude/longitude coordinates ...', and 'Choose location on map ...'. The 'Choose location on map ...' option is selected, and a map of Europe is displayed with a red crosshair indicating a location in the UK. Below the map is an 'Update Location' button. At the bottom, there is a 'Delete Location' section with a 'Delete Location' button and a 'Confirm' checkbox.

5. Click **Update Location** to save your changes.
6. Repeat this procedure for each PCS endpoint you want to load-balance.

Creating GLB Location Monitors

The Traffic Manager uses Health Monitors to monitor the status of your GLB Locations and to inform the load-balancing decision for each incoming request.

For each of your GLB Locations, create a new "Pool/GLB Monitor" and instruct it to monitor the IP address or hostname of the PCS instance at that location.

To create a new monitor, perform the following steps:

1. In the Traffic Manager Admin UI, click **Catalogs > Monitors**.
2. In the "Create new monitor" section, enter the following:
 - **Name:** The name for this Service Monitor. For identifying purposes, use a name that corresponds to the name of a GLB Location.
 - **Type:** Choose the monitor type that best suits your requirements. For this example, select "HTTP monitor".
 - **Scope:** Select "Pool/GLB" and enter the IP address and port of the PCS service present at the GLB Location you want to monitor. For example, if this monitor is intended for the location hosting "vpn-eu.test.pulsesecure.net", type "192.0.2.2:443" to represent the IP address and port associated with the PCS service.

FIGURE 10 Adding a GLB location monitor

Create new monitor

Name:

The internal monitor implementation of this monitor.

type:

- Ping monitor
- TCP Connect monitor
- HTTP monitor
- TCP transaction monitor
- External program monitor ...
- SIP monitor
- RTSP monitor

A monitor can either monitor each node in the pool separately and disable an individual node if it fails, or it can monitor a specific machine and disable the entire pool if that machine fails. GLB location monitors must monitor a specific machine.

scope:

- Node: Monitor each node in the pool separately
- Pool/GLB: Monitor a specified machine ...

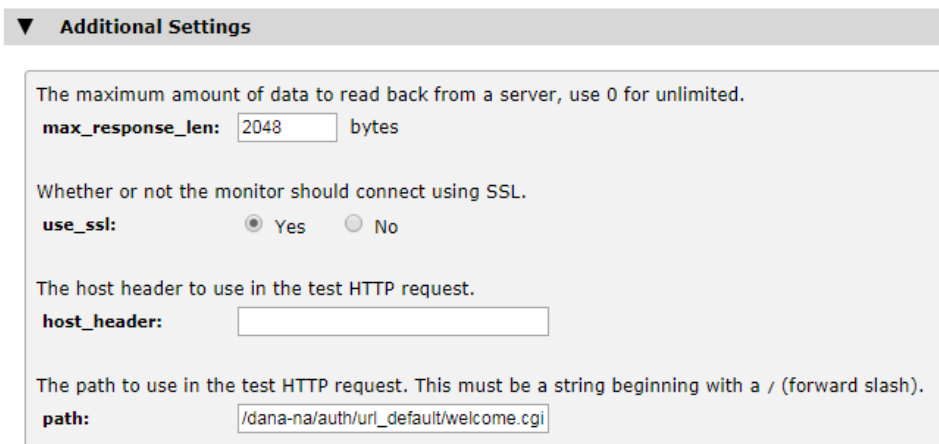
IP or hostname to monitor

3. Click **Create Monitor** to create this Service Monitor and access the edit page.
4. On the monitor edit page, under "Additional Settings", make sure **use_ssl** is set to "Yes". Then add the following to the path field:

```
/dana-na/auth/url_default/welcome.cgi
```

The HTTP test is performed against this path.

FIGURE 11 Modifying monitor settings



▼ **Additional Settings**

The maximum amount of data to read back from a server, use 0 for unlimited.

max_response_len: bytes

Whether or not the monitor should connect using SSL.

use_ssl: Yes No

The host header to use in the test HTTP request.

host_header:

The path to use in the test HTTP request. This must be a string beginning with a / (forward slash).

path:

5. click **Update** to save the changes.
6. Repeat this procedure for each GLB Location you want to monitor. For ease of use, use the "Copy Monitor" feature on the Monitor Edit page to quickly duplicate monitor configuration.

Creating a GLB Service

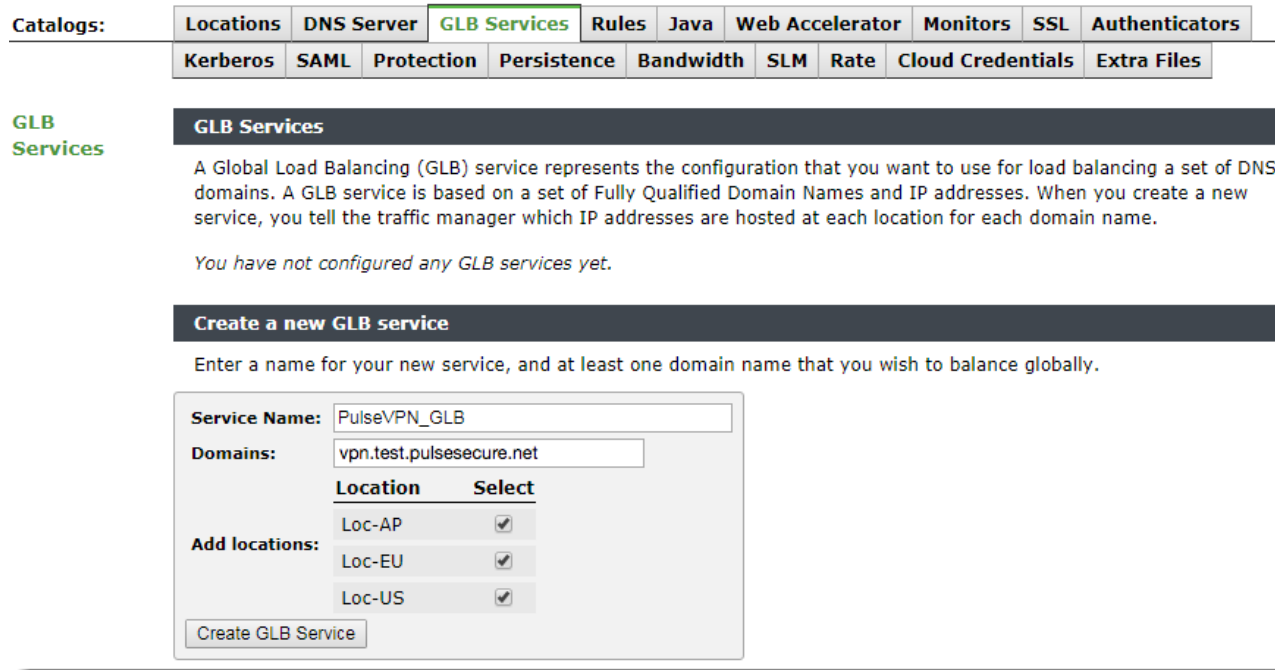
A GLB service represents the global load balancing configuration that you want to use for a set of DNS domains. The GLB service links to the GLB locations you defined previously, and contains the load-balancing and monitoring logic used to determine the response to a DNS request for a given set of conditions.

This procedure assumes you have already created GLB Locations and Health Monitors for each PCS endpoint.

To create a GLB service, perform the following steps:

1. In the Traffic Manager Admin UI, click **Catalogs > GLB Services**.
2. In the "Create a new GLB service" section, enter the following:
 - **Service Name:** The identifying name for this GLB service.
 - **Domains:** Enter the fully qualified domain names you want this GLB service to balance globally. For this example, use the unified endpoint URL "vpn.test.pulsesecure.net".
 - **Add locations:** Select all the previously-defined GLB Locations you want to load balance against the domain.

FIGURE 12 Creating a GLB Service



3. Click **Create GLB Service** to create this GLB Service and access the edit page.

When the Traffic Manager receives an incoming client request, it uses the GLB service to identify and determine if a suitable GLB Location is available to use. If such a location is identified, it returns the IP address allocated to the location. Therefore, each location connected to the GLB service must have assigned to it:

- The IP addresses on which the services hosted there are running.
- A corresponding GLB location health monitor.

For the purposes of this guide, the IP addresses are those assigned to the individual PCS location hostnames in your DNS zone file, and the health monitors are those created in the previous section.

To set up IP addresses and health monitors, perform the following steps for each location added to your GLB Service:

1. In the GLB Service edit page, click **Locations and Monitoring**.
2. For each location, set **Service IP Address** to the corresponding address from your zone file. For example, if your PCS instance at "vpn-us.test.pulsesecure.net" corresponds to a defined GLB Location, set that location's Service IP Address to "192.0.2.1".
3. For **Monitors**, select the correspondingly-named monitor from the drop-down list.

FIGURE 13 Configuring service IP addresses and health monitors for the “Loc-AP” location

4. Click **Update** to save your changes.
5. Repeat this process for each location.

Before you can use this GLB Service, make sure the load balancing algorithm is suitable for your requirements. In most cases, the default "Adaptive" option provides the best traffic distribution model based on a combination of current load and geographic location. To select an alternative method, click **Load Balancing** from the GLB Service edit page.

FIGURE 14 Selecting a load balancing algorithm for this GLB service

Load
Balancing

GLB Service: PulseVPN_GLB Unfold All / Fold All

Load Balancing settings control how traffic is distributed between locations.

Defines the global load balancing algorithm to be used.

algorithm:

- Load ...
- Geographic
- Adaptive ...
- Geo Effect: %
- Round Robin
- Weighted Random ...
- Primary/Backup ...

Locations:

- ▶ Loc-AP
- ▶ Loc-EU
- ▶ Loc-US

Locations recovering from a failure will become disabled.

disable_on_failure: Yes No

The last location to fail will be available as soon as it recovers.

autorecovery: Yes No

The response to be sent in case there are no locations available.

last_resort_response:

For a full description of how each algorithm affects the load balancing decision, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

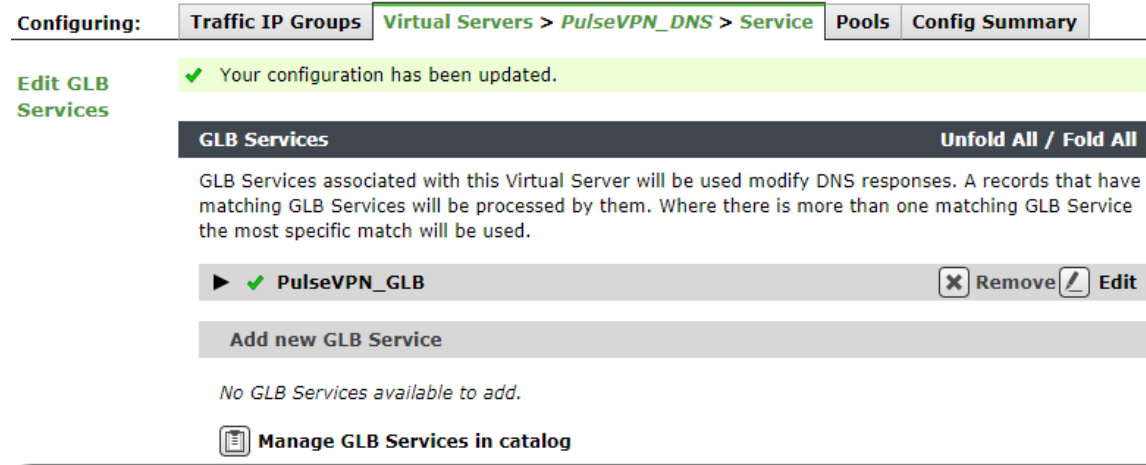
The new GLB service is created in a disabled state. In the edit page, set **Enabled** to "Yes".

Adding GSLB Functionality to your Traffic Manager DNS Service

After you have created your GLB Service configuration, complete with fully monitored PCS endpoint locations, attach the GLB Service to your DNS virtual server. Perform the following steps:

1. In the Traffic Manager Admin UI, click **Services > Virtual Servers** and then click the name of your DNS virtual server.
2. In the virtual server edit page, click **GLB Services**.
3. Select your GLB Service from the drop-down list and click **Add Service**.

FIGURE 15 Adding a GLB Service to a virtual server



If your DNS virtual server is already enabled, GSLB commences immediately. Check the “Event Log” or “Cluster Diagnosis” page for indications of any problems with the configuration.