



Load Balancing Microsoft SharePoint 2016 with Pulse Secure Virtual Traffic Manager

Deployment Guide

Published **15 December, 2018**

Document Version **1.0**

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

www.pulsesecure.net

© 2018 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.

Load Balancing Microsoft SharePoint 2016 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
IMPLEMENTATION OVERVIEW.....	1
CONFIGURING THE TRAFFIC MANAGER.....	5
BEFORE YOU BEGIN.....	5
SETTING UP A LOAD-BALANCING SERVICE.....	5
ADDING AN SSL CERTIFICATE.....	8
ENABLING SSL DECRYPTION FOR YOUR SHAREPOINT 2016 SERVICE.....	9
ASSIGNING A TRAFFIC IP ADDRESS TO YOUR SERVICE.....	10
OPTIONAL CONFIGURATION TO ENHANCE YOUR SERVICE.....	13
USING HTTP/2 TO INCREASE PERFORMANCE.....	13
MONITORING THE HEALTH OF YOUR SHAREPOINT 2016 SERVER FARM.....	14
FURTHER HEALTH MONITORING.....	14
CONTENT CACHING.....	16
HTTP TO HTTPS REDIRECTS.....	17
CONTENT COMPRESSION.....	19
BANDWIDTH MANAGEMENT.....	20
SECURITY ENHANCEMENTS.....	21
CONCURRENT CONNECTIONS.....	22
CONNECTION RATE.....	22
ACCESS RESTRICTIONS.....	22

Introduction

Purpose of this Guide

This guide describes how to configure Pulse Secure Virtual Traffic Manager (the Traffic Manager) to load balance traffic to a farm of Microsoft SharePoint 2016 web front-end server nodes.

The Traffic Manager can be deployed for SharePoint 2016 to increase performance, enhance user experience, control service levels, reduce cost on application servers, and add security features to the deployment.

Prerequisites

This guide deals primarily with the steps required to configure your Traffic Manager.

This guide assumes you are familiar with Microsoft SharePoint 2016, that you have previously configured a SharePoint 2016 on-premise server farm, and have configured the required Alternative Access Mappings and Internet Information Services (IIS) bindings for your SharePoint service.

To learn more about setting up SharePoint 2016, see <https://docs.microsoft.com/en-us/sharepoint/getting-started>.

The deployment scenario described in this guide was tested with Pulse Secure Virtual Traffic Manager 18.2. For full details of how to install and configure the Traffic Manager, see the *Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide* applicable to your product variant, available from the Pulse Secure Technical Publications website <https://www.pulsesecure.net/techpubs/Pulse-vADC-Solutions/Pulse-Virtual-Traffic-Manager>.

You administer all Traffic Manager variants through a web-enabled user interface known as the Admin UI. The Traffic Manager supports the following browsers for this purpose:

- Internet Explorer: v.11 or newer
- Microsoft Edge: latest version
- Mozilla Firefox: latest version
- Apple Safari: latest version
- Google Chrome: latest version

Implementation Overview

The implementation described in this guide consists of two SharePoint 2016 web front-end (WFE) servers deployed together in a farm with an application server and SQL database. This server farm should expose two WFE endpoints, to which the Traffic Manager balances traffic. Each endpoint becomes a back-end server node in the Traffic Manager's SharePoint 2016 pool configuration.

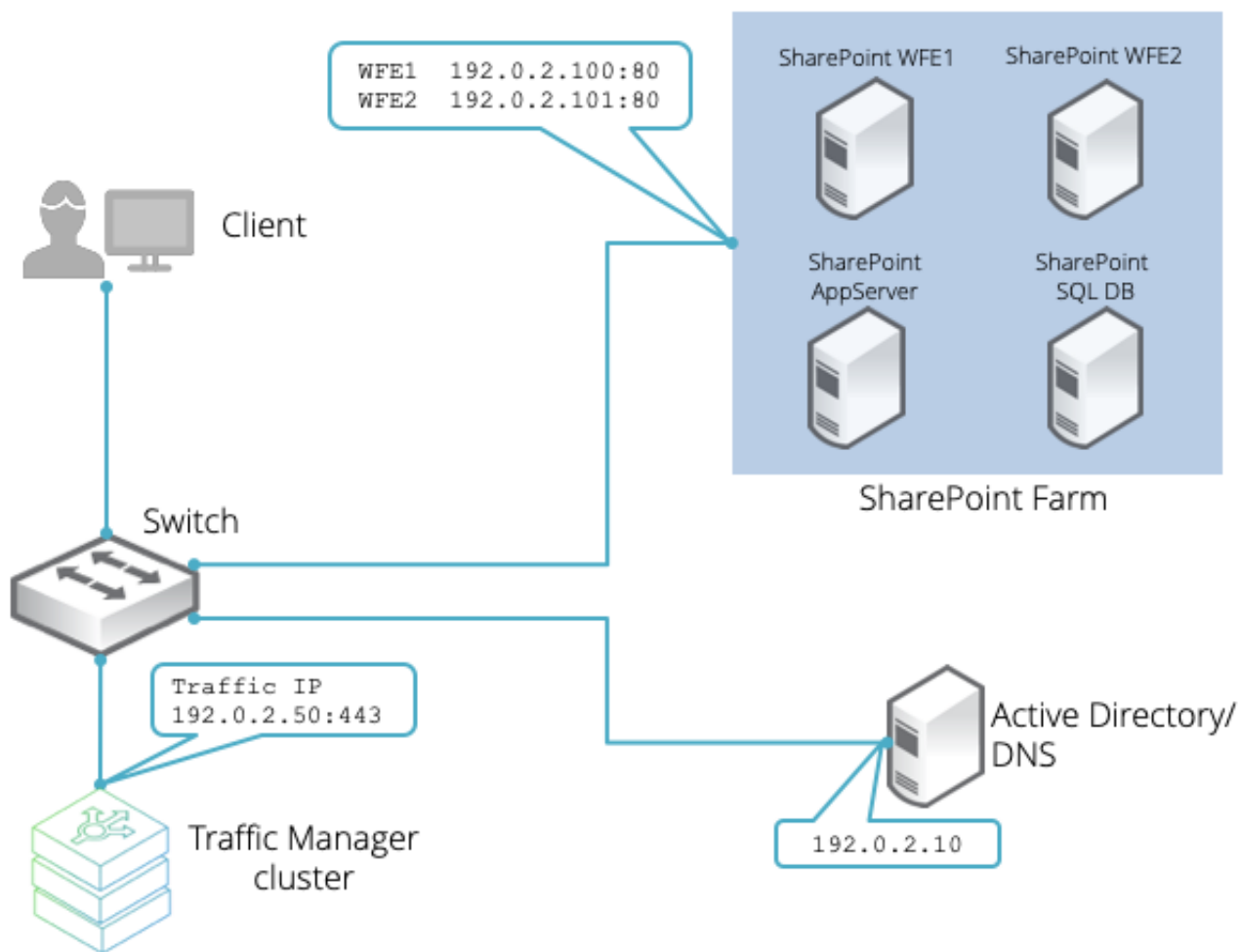
Note: To increase the performance and resilience of your SharePoint 2016 service, consider deploying additional SharePoint 2016 WFE instances and add them to the Traffic Manager pool.

The Traffic Manager is best deployed as a fault-tolerant cluster, although a single Traffic Manager instance can provide the same load-balancing and traffic management capabilities. Where a Traffic Manager cluster is employed, Pulse Secure advises raising a Traffic IP address (TIP) to act as a single SharePoint service endpoint for the client. The Traffic Manager accepts client connections to the TIP and balances requests across the WFE server nodes configured in the SharePoint pool.

Note: To learn more about the Traffic Manager terminology used in this guide, such as Traffic IP addresses, virtual servers, and pools, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

An Active Directory (AD) server provides DNS and authentication services.

Figure 1 Network topology for load-balancing a SharePoint 2016 server farm



This configuration offers the following benefits:

- SharePoint 2016 connectivity over a secure (HTTPS) connection.
- Health monitoring of SharePoint 2016 servers so that traffic is sent only to healthy servers in the pool.

- Automatic redirection of end user sessions between HTTPS and HTTP (Port 443 and port 80).
- Content caching optimizes back-end server access and allows faster access to common documents.
- Optimization of TCP connections to the Traffic Manager, minimizing network latency and traffic delay problems.
- All users must enter their credentials based on Active Directory details in order to access SharePoint 2016 services.
- All users must accept the SSL certificate when offered within the browser.

Configuring the Traffic Manager

Before you Begin

Make sure you have performed all of the following actions prior to setting up your Traffic Manager SharePoint 2016 load-balancing service:

- Install and configure a fully functioning SharePoint 2016 server farm according to the deployment topology described in this guide, including Active Directory (AD) services.
- Install and configure a cluster of two or more Traffic Managers in the same subnet as the SharePoint 2016 server farm.
- Install full licenses for all components.
- Understand Alternative Access Mappings for the SharePoint 2016 Server (Zones Configuration).
- Designate client workstations to test access to the deployment (through the same subnet or routed access).

Setting up a Load-Balancing Service

This section describes how to create a new service on the Traffic Manager to load-balance traffic to your SharePoint 2016 server farm.

Before you start the process, make sure you have the following details:

- The IP address and port of the management interface on one of your Traffic Managers.
- The administrator username and password for your Traffic Manager cluster.
- The IP addresses and ports of your SharePoint 2016 web front-end (WFE) endpoints.
- The IP address you want your clients to use to access the SharePoint 2016 service (the Traffic IP address).

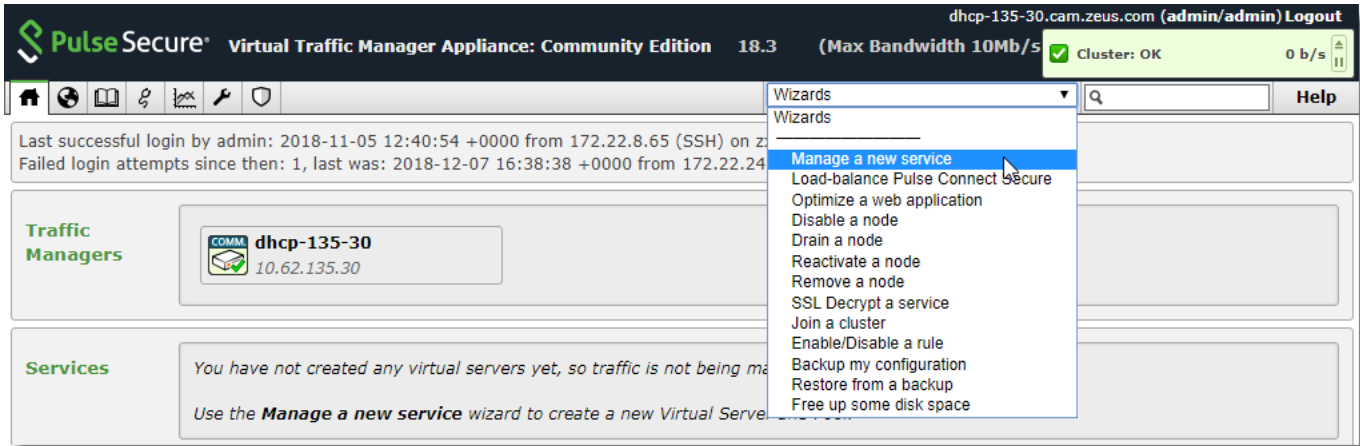
To set up the new service, perform the following steps:

1. In a web browser, navigate to the IP address and port of your Traffic Manager Administration Interface (the Admin UI). For example, "http://192.0.2.1:9090".

Due to the way that Traffic Manager cluster members share configuration, you can use the Admin UI of any one of your Traffic Managers to create the new service, and the configuration is automatically replicated out to all other cluster members.

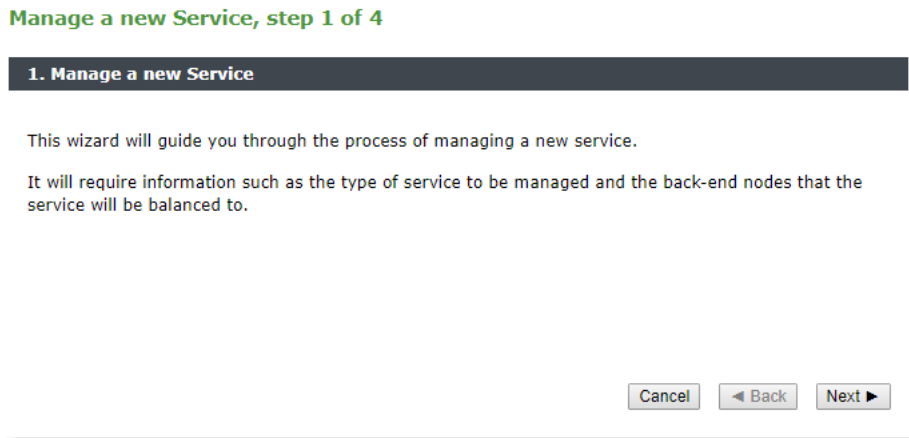
2. Log in to the Traffic Manager Admin UI with the administrator credentials.
3. From the Home page, select **Manage a new service** from the "Wizards" drop-down list (in the tool bar):

Figure 2 Running the "Manage a new service" wizard



4. The Traffic Manager displays the first page of the Manage a new service wizard in a new window:

Figure 3 Manage a new service wizard, step 1



To continue to the next step, click **Next**.

To quit the wizard without making any changes, click **Cancel**.

Figure 4 Manage a new service wizard, step 2

2. Specify the service

Please enter a brief name to identify the service you would like to balance.

Name:

Please select the protocol that the service uses.

Protocol:

Please specify the port that the protocol listens on.

Port:

5. Enter a name for the new service, set the protocol to HTTP, and enter 443 as the port number.

To continue to the next step, click **Next**.

Figure 5 Manage a new service wizard, page 3

3. Specify the back-end nodes

Please enter the hostname and port of each node:

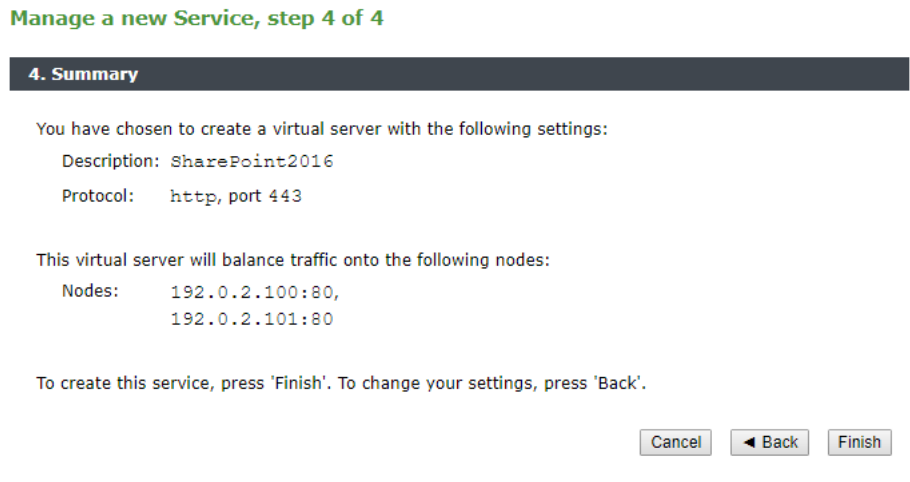
Hostname: Port:

Nodes:

To remove a node from the list, select it and press 'Remove node':

6. Enter the IP address or hostname of your first SharePoint 2016 WFE endpoint, enter 80 as the port number, then click **Add Node**.
7. Repeat this step for the second WFE endpoint.
8. To continue to the next step, click **Next**.

Figure 6 Manage a new service wizard, page 4



9. Check that the settings shown are correct, then click **Finish** to close the wizard and create the new service.

To go back to the previous step, click **Back**. To cancel the wizard without making any changes, click **Cancel**.

Note: The service you create uses the default *Round Robin* load-balancing algorithm. To use an alternative algorithm, click **Pool > SharePoint2016 > Load Balancing**.

Adding an SSL Certificate

Your new service requires an SSL certificate to decrypt incoming connections before they are passed on to the SharePoint 2016 back-end. The Traffic Manager includes the ability to import an existing SSL certificate, or to generate your own self-signed certificate:

- To import an existing certificate, click **Catalogs > SSL > Server Certs > Import Certificate**. Use this page to upload your certificate and private key files to the Traffic Manager.
- To generate a new self-signed certificate, perform the following steps:
 1. Click **Catalogs > SSL > Server Certs > Create Self-Signed Certificate / Certificate Signing Request**.
 2. Enter the details of your self-signed certificate into the form provided. Pulse Secure recommends using a 2048-bit key type as a minimum.

Figure 7 Creating a self-signed SSL certificate

Enter a short name to identify your certificate. If you leave this blank, the 'Common Name' field or the first 'Subject Alternative Name' will be used.

Name:

List DNS names and IP addresses to include them in the certificate's Subject Alternative Name extension.

Subject Alternative Name(s):

The public DNS address of your server, such as 'secure.yourcompany.com':

Common Name (CN):

The name of your organization, such as 'Your Company':

Organization (O):

The unit within your organization, such as 'Sales':

Organizational Unit (OU): (optional)

Your location (town or city), such as 'Anytown':

Location (L):

Your state or province, such as 'Somestate':

State (S): (required for US only)

Your two-letter country code, such as 'US', 'GB' or 'FR':

Country (C):

How long should this certificate be valid for:

Expires in: ▼

Private key type (2048 bit RSA or P-256 ECDSA recommended):

Key type: ▼

3. Click **Create certificate**.

For more information concerning the creation of SSL certificates, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Enabling SSL Decryption for your SharePoint 2016 Service

The SharePoint 2016 service you configure in this guide is set up to accept secure HTTPS connections on port 443, and to subsequently load-balance traffic to the unsecured WFE endpoints on HTTP port 80. To decrypt connections as they pass through the Traffic Manager, enable the *SSL Decryption* feature and add your SSL server certificate to the SharePoint 2016 service.

To enable SSL decryption for your SharePoint 2016 service, perform the following steps:

1. Click **Services > Virtual Servers > (SharePoint 2016 service name) > SSL Decryption**.

Figure 8 Enabling SSL decryption for SharePoint 2016 client connections

SSL Decryption

These settings control how SSL connections are decrypted.

Whether or not the virtual server should decrypt incoming SSL traffic.

ssl_decrypt: Yes No

Which SSL certificate(s) should this virtual server use?
 Additional certificates can be supplied to match different sites hosted by this virtual server. You can specify a different certificate for any hostname or IP address. The wildcard character '*' can be used to match multiple hostnames. If none of the addresses or hostnames match the default certificate will be used.

Note: Hostname mappings require support of the TLS 1.0 'Server Name Indication' extension, which is not supported by all browsers.


certificate: Default Certificates: SP2016 (secure.example.com, Expires 10 Dec 2019, RSA) ▼

alt_certificates: Select a certificate... ▼

Add certificate mapping:

IP Address / Host Name:

Certificates: Select a certificate... ▼
Select a certificate... ▼

 **Manage SSL Certificates**

Whether or not the virtual server should add HTTP headers to each request to show the SSL connection parameters.

ssl_headers: Yes No

If the traffic manager is receiving traffic sent from another traffic manager, then enabling this option will allow it to decode extra information on the true origin of the SSL connection. This information is supplied by the first traffic manager.

ssl_trust_magic: Yes No

Whether or not to send an SSL/TLS "close alert" when the traffic manager is initiating an SSL socket disconnection.

ssl_send_close_alerts: Yes No

If OCSP URIs are present in certificates used by this virtual server, then enabling this option will allow the traffic manager to provide OCSP responses for these certificates as part of the handshake, if the client sends a TLS status_request extension in the ClientHello.

ssl_ocsp_stapling: Yes No

2. Make sure your SSL certificate is selected in the **certificate** field.
3. Set **ssl_decrypt** to "Yes".
4. To save your changes, click **Update** in the "Apply Changes" section.

Assigning a Traffic IP Address to your Service

To ensure full service availability, your Traffic Manager instances in the same cluster can be configured to share one or more defined Traffic IP addresses (TIPs). TIPs are not tied to any one Traffic Manager instance and the whole cluster works to ensure that each TIP is fully available, even if some of the Traffic Managers have failed. You then configure your DNS to resolve the SharePoint 2016 service URL to the TIPs raised in your cluster.

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

Traffic IP addresses are organized into Traffic IP groups, with a group consisting of one or more TIPs managed across one or more cluster members.

To create and assign a TIP to your Traffic Manager cluster for your SharePoint 2016 service, perform the following steps:

1. Click **Services > Traffic IP Groups**.
2. In the "Create a new Traffic IP Group" section, enter an identifying name for your new group.
3. Select the Traffic Managers across which the TIPs should be distributed.
4. Enter one or more IP addresses you want to define as TIPs in this group. Use a space- or comma-separated list.
5. Choose the IP distribution mode you want to use for this group. For advice on the mode most appropriate to your circumstances, see the UI Help or refer to the *Pulse Secure Virtual Traffic Manager: User's Guide*.
6. Click **Create Traffic IP Group**.
7. Configure your DNS to resolve the fully-qualified URL of your SharePoint 2016 service to all of the TIPs defined in the Traffic IP group.

Optional Configuration to Enhance your Service

To enhance the performance and security of your deployment, the Traffic Manager offers a number of optional capabilities that you can apply to your SharePoint 2016 service configuration:

- **“Using HTTP/2 to Increase Performance”**: improves performance by configuring the Traffic Manager to handle HTTP/2 traffic from clients.
- **“Monitoring the Health of your SharePoint 2016 Server Farm”**: enables the Traffic Manager to detect if a SharePoint 2016 web front-end (WFE) has failed, to suspend traffic to that WFE instance, and to re-introduce the WFE gracefully after it has recovered.
- **“Content Caching”**: allows caching of common content to enhance performance.
- **“HTTP to HTTPS Redirects”**: makes sure HTTP requests are always redirected to HTTPS.
- **“Content Compression”**: enables the Traffic Manager to compress HTTP responses to the client in order to reduce bandwidth usage and increase speed of delivery.
- **“Bandwidth Management”**: allows the Traffic Manager to limit the number of bytes per second used by inbound or outbound traffic.
- **“Security Enhancements”**: filters unwanted web requests and protects your applications from external threats.

Note: This chapter provides an introduction to each feature with respect to how it might apply to your SharePoint 2016 service. For a more detailed description of all Traffic Manager features and capabilities, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Using HTTP/2 to Increase Performance

The Traffic Manager offers client-side support for the HTTP/2 protocol (see RFC7540 and RFC7541). HTTP/2 is intended as a replacement for HTTP/1.x and is designed to improve page-load times over high latency connections, most notably by supporting transaction multiplexing over a single TCP connection.

HTTP requests received over HTTP/2 connections are translated into HTTP/1.1 format before being processed by the Traffic Manager and load-balanced across the SharePoint 2016 pool. As such, your SharePoint 2016 WFE server nodes do not need to support HTTP/2 to have this feature enabled on the Traffic Manager.

ATTENTION

HTTP/2 over a secure connection requires TLSv1.2 or later, the `SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256` cipher, the P256 elliptic curve, and does not support renegotiation after connection establishment. These options are enabled by default, but might have been disabled after upgrading your Traffic Manager from an older release. Clients using an obsolete cipher or older TLS version can only send HTTP/1.x requests when connecting to a virtual server with HTTP/2 enabled.

To enable HTTP/2, click **Services > Virtual Servers > (SharePoint 2016 VS name) > Protocol Settings > HTTP/2-Specific Settings**. Set `https!enabled` to "Yes", then click **Update** to save your changes.

Monitoring the Health of your SharePoint 2016 Server Farm

Your SharePoint 2016 service in the Traffic Manager includes, as standard, health monitoring in the form of a Ping monitor. This means that the Traffic Manager periodically sends a Ping request to each node in the SharePoint 2016 server pool to determine basic connectivity. If a node does not respond to the Ping, it is marked as unavailable and requests are shared between all other live nodes.

The Traffic Manager continues to perform the connectivity test against the unavailable node, with decreasing regularity. If the node recovers, the Traffic Manager seamlessly recommences sending requests.

To modify the parameters for the Ping monitor, click **Catalogs > Monitors > Ping**.

Further Health Monitoring

The Traffic Manager includes the option to add more advanced health monitoring to your SharePoint 2016 service in the form of live traffic requests to each node, designed to detect a wider range of errors.

To add live traffic requests, use a "Full HTTP" monitor. This monitor requests a specified page from a server node and looks for a suitable status code in the response. However, end users might experience slow or broken responses while the health monitor seeks to confirm that the node has failed.

To add a Full HTTP monitor to your SharePoint 2016 server pool, click **Services > Pools > (SharePoint 2016 pool name) > Health Monitoring**.

Figure 1 Adding a Full HTTP health monitor

The screenshot shows the configuration page for a pool named "SharePoint2016 (HTTP, 2 nodes)". The breadcrumb navigation is "Pools > SharePoint2016 > Monitors". The page has tabs for "Traffic IP Groups", "Virtual Servers", "Pools > SharePoint2016 > Monitors", and "Config Summary". On the left, there is a sidebar with "Edit Monitors". The main content area has a header "Pool: SharePoint2016 (HTTP, 2 nodes)" and "Unfold All / Fold All". Below this is a "Monitors" section with a description: "Monitors watch the nodes in a pool, and inform the traffic manager if the nodes are functioning correctly." There is a "Ping" monitor listed with "Remove" and "Edit" buttons. The "Add monitor:" section has a dropdown menu open, showing options: Client First, Client First, Connect, DNS, FTP, Full HTTP (highlighted), Full HTTPS, POP, RTSP, Server First, Simple HTTP, Simple HTTPS, SIP TCP, SIP TLS, SIP UDP, and SMTP. There is an "Add Monitor" button and a "Manage Monitors in Catalog" link. Below the dropdown, there is a "Passive monitor" section with a checkbox and a "No" radio button. At the bottom, there are "Apply Changes" and "Update" buttons.

Locate the "Add monitor" section and select "Full HTTP" from the monitor drop-down list, then click **Add Monitor**.

Next, edit the Full HTTP monitor to include settings specific to your SharePoint 2016 deployment. Click the monitor name or click the **Edit** link to the right.

On the Full HTTP monitor settings page, locate the "Additional Settings" section.

Figure 2 Editing the Full HTTP monitor additional 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:

The HTTP basic-auth <user>:<password> to use for the test HTTP request.
authentication:

A regular expression that the HTTP status code must match. If the status code doesn't matter then set this to .* (match anything).
status_regex:

A regular expression that the HTTP response body must match. If the response body content doesn't matter then set this to .* (match anything).
body_regex:

Enter the `host_header`, `path`, and `HTTP basic-auth` authentication credentials that the Traffic Manager should use in the HTTP GET request to the SharePoint 2016 WFE. This example performs active health monitoring by authenticating into the SharePoint 2016 application using a dedicated SharePoint account "monitoruser".

For more details about health monitoring, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Content Caching

A Traffic Manager HTTP virtual server can detect commonly requested HTTP resources, and remember their content if it does not change each time it is requested. When a virtual server sees a further request for the same resource, it can return the content for the resource directly from the local cache. This capability reduces the load on your SharePoint 2016 servers and improves the performance and capacity of your SharePoint 2016 service.

To enable Content Caching for your SharePoint 2016 service, click **Services > Virtual Servers > (SharePoint 2016 VS name) > Content Caching**.

Figure 3 Enabling Content Caching

Configuring: [Traffic IP Groups](#) [Virtual Servers > SharePoint2016 > Content Caching](#) [Pools](#) [Config Summary](#)

Content Caching

Virtual Server: SharePoint2016 (HTTP, port 443)

Web pages generated by your web servers can be cached to speed up your services.

Caching settings

These settings control what is cached by this virtual server.

If set to **yes** the traffic manager will attempt to cache web server responses.

webcache!enabled: Yes No

Maximum time period to cache web pages for.

webcache!time: seconds

Time period to cache error pages for.

webcache!errorpage_time: seconds


The "Cache-Control" header to add to every cached HTTP response, `no-cache` or `max-age=600` for example.

webcache!control_out:


If a cached page is about to expire within this time, the traffic manager will start to forward some new requests on to the web servers. A maximum of one request per second will be forwarded; the remainder will continue to be served from the cache. This prevents "bursts" of traffic to your web servers when an item expires from the cache. Setting this value to `0` will stop the traffic manager updating the cache before it expires.

webcache!refresh_time: seconds

You can see what pages are in the cache on the [Activity > Content Cache](#) page.

 **View cache contents**

Controls for the global cache size can be found on the [System > Global Settings](#) page.

 **Modify global cache size**

To enable caching, set **webcache!enabled** to "Yes" and click **Update**.

HTTP to HTTPS Redirects

To ensure that users all access the SharePoint 2016 portal securely, Pulse Secure recommends configuring a redirect from HTTP Port 80 to HTTPS port 443.

To implement the redirect, create a new Virtual Server listening on the same Traffic IP address as the main SharePoint 2016 service, but at HTTP port 80. This virtual server does not require an assigned back-end pool so set the default pool to "discard".

The new HTTP Virtual Server uses a TrafficScript *Request Rule* to complete the redirect. To create the rule, click **Catalogs > Rules** and enter your rule name in the "Create new rule" section. Then, select "Use TrafficScript Language" and click **Create Rule**. In the rule edit page that follows, add the following code line:

```
http.changeSite("https://" . http.getHeader ( "Host"));
```

Figure 4 Creating a redirect TrafficScript rule

The screenshot shows the Pulse Secure Virtual Traffic Manager interface. The top navigation bar includes 'Catalogs:' followed by tabs for 'Locations', 'DNS Server', 'GLB Services', 'Rules > SP2016_redirect', 'Java', 'Web Accelerator', and 'Monitors'. Below this are sub-tabs for 'SSL', 'Authenticators', 'Kerberos', 'SAML', 'Protection', 'Persistence', 'Bandwidth', 'SLM', and 'Rate'. Further down are 'Service Discovery', 'Cloud Credentials', and 'Extra Files'.

A green notification bar at the top of the main content area states: '✓ Your configuration has been updated.'

The main content area is titled 'Rule: SP2016_redirect'. It contains a form with the following fields:

- Name:** SP2016_redirect
- Notes:** (empty text area)
- Rule:** A code editor containing the following TrafficScript code:


```
1 http.changeSite("https://" . http.getHeader ( "Host"));
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
```

At the bottom of the form are two buttons: 'Update' and 'Check Syntax'.

To add the rule to your redirecting Virtual Server, click **Services > Virtual Servers > (redirect VS name) > Rules**. Locate the "Request Rules" section and select the redirect rule from the drop-down list. To complete the procedure, click **Add Rule**.

Figure 5 Adding a request rule to a Virtual Server

Configuring: [Traffic IP Groups](#) [Virtual Servers > SP2016_redirect > Rules](#) [Pools](#) [Config Summary](#)

Edit Rules **Virtual Server: SP2016_redirect (HTTP, port 80)**

TrafficScript rules are evaluated in order. If a rule selects a pool, the request is balanced by that pool, and no more rules are evaluated. If no pool is selected, the request is balanced by the default traffic pool.

Request Rules

Request rules are evaluated before the request is sent to the pool.

No rules have been configured for this virtual server

Add rule:

Response Rules

Response rules are evaluated after the server responds to a request.

No rules have been configured for this virtual server

Add rule:

Transaction Completion Rules

Transaction completion rules are evaluated at the end of the transaction, for example when the connection is closed or when a complete HTTP, SIP, or RTSP response has been sent to the client.

No rules have been configured for this virtual server

Add rule:

Note: Make sure the rule is marked as *enabled* in the Virtual Server.

Content Compression

The Traffic Manager can compress the HTTP response it sends to a remote client. This can reduce your bandwidth usage, and speed up the delivery of large Web pages to clients with slow connections.

Not all browsers can receive compressed content; those which do specify this in the HTTP request headers. The Traffic Manager compresses content only for those browsers which are able to decompress it.

To enable content compression for your SharePoint 2016 service, click **Services > Virtual Servers > (SharePoint2016 VS name) > Content Compression**. On this page, set **gzip!enabled** to "Yes", then click **Update** to apply your changes.

Figure 6 Enabling content compression for a virtual server

The screenshot shows the configuration page for a virtual server named "SharePoint2016 (HTTP, port 443)". The breadcrumb navigation is "Virtual Servers > SharePoint2016 > Content Compression". The page has tabs for "Traffic IP Groups", "Virtual Servers > SharePoint2016 > Content Compression", "Pools", and "Config Summary".

Under the "Content Compression" section, there is a header "Virtual Server: SharePoint2016 (HTTP, port 443)" and a link "Unfold All / Fold All". Below this, a text box states: "These settings configure how the virtual server compresses the content it returns to the browser."

The first setting is "Compress web pages sent back by the server." with the label **gzip!enabled:** and two radio buttons: "Yes" (selected) and "No".

Below this is a section titled "Compression settings" with a sub-header "You can control your compression parameters using the settings in this section."

The "Compression settings" section contains a text box with the following settings:

- Compression level (1-9, 1=low, 9=high). **gzip!compresslevel:** Level 1
- Maximum document size to compress (0 means unlimited). **gzip!maxsize:** 10000000 bytes
- Minimum document size to compress. **gzip!minsize:** 1000 bytes
- Compress documents with no given size. **gzip!nosize:** Yes (selected) No

To control the level of compression applied, set **gzip!compresslevel** to a value between 1 and 9. A lower value applies less compression to your data and uses less CPU time. A higher value means a greater level of compression, but with higher CPU usage resulting in reduced Traffic Manager performance.

Bandwidth Management

The Traffic Manager uses bandwidth classes to limit the network resources that a set of connections can consume. By apply a bandwidth class to your SharePoint 2016 service, you can limit the bandwidth used when sending data to clients.

Note: Make sure you select a bandwidth limit that fits your organizational policies, as an excessive limit can inadvertently cap throughput and access for users at peak periods.

To create a bandwidth class, click **Catalogs > Bandwidth classes**. Type a name into the "Create new bandwidth class" section and click **Create Class**.

Figure 7 Creating a bandwidth class

Catalogs: Locations DNS Server GLB Services Rules Java Web Accelerator Monitors SSL Authenticators Kerberos SAML

Protection Persistence **Bandwidth > SP2016_bw** SLM Rate Service Discovery Cloud Credentials Extra Files

Bandwidth Management Catalog

Class: SP2016_bw Unfold All / Fold All

SP2016_bw is currently not being used by any virtual servers, rules or pools.

Last Modified: 13 Dec 2018 15:53

Basic Settings

These settings control how this Bandwidth class throttles the network traffic.

Name: SP2016_bw

The maximum bandwidth to allocate to connections that are associated with this bandwidth class (in kbits/second).

maximum: 10 Mbit 10000 kbits/second

The scope of the bandwidth class.

sharing: Bandwidth is shared across all traffic managers

A description of this bandwidth class.

note:

In the class edit page, set "maximum" to the bandwidth limit you require, and set "sharing" to define the scope. Click **Update** to apply your changes.

After you have created the bandwidth class, apply it to your SharePoint2016 Virtual Server by clicking **Services > Virtual Servers > (SharePoint 2016 VS name) > Classes > Bandwidth Management**. Select the new class and click **Update** to save the changes.

Security Enhancements

The Traffic Manager offers a number of additional features to protect, control, and enhance the user experience. Pulse Secure recommends configuring these features as applicable to your organizational needs.

The Traffic Manager's *Service Protection* system can be configured to screen all incoming requests so that any matching specified criteria are dropped. This functionality can be used to protect your SharePoint 2016 services against known vulnerability exploit attacks and malicious access attempts.

To incorporate protection, create a Service Protection class and apply it to your SharePoint 2016 virtual server. Click **Catalogs > Protection** and create a new Service Protection class called "SharePoint_Security" (or whatever name suits your requirements). Then, add the class to your virtual server by clicking **Services > Virtual Servers > (SharePoint 2016 VS name) > Classes > Service Protection**. Select the new class and click **Update** to save the changes.

A Service Protection class offers many different categories of protection. Useful protection categories are described below. Edit the class and locate the appropriate category to reveal the applicable settings.

Concurrent Connections

This feature allows the Traffic Manager to limit the total number of concurrent connections each connecting IP address is allowed. This is useful if your network bandwidth is limited and you want to control the total number of concurrent users in a given timeframe.

To set a maximum number of connections per IP address, click **Catalogs > Protection > *SharePoint_Security* > Concurrent Connections**. Set **max_1_connections** to a value according to your needs.

Connection Rate

Use this feature to limit the rate at which each connecting IP address can make new connections or requests. Set the maximum number of connections, and the time period within which the connections can be made.

To configure a connection rate, click **Catalogs > Protection > *SharePoint_Security* > Connection Rate**.

Access Restrictions

The source IP address of a client can be used to decide whether or not to accept requests. If a particular IP address or network block is generating malicious requests, the Traffic Manager can be configured to drop all connections from these addresses, thus protecting the SharePoint 2016 server pool from attack.

To configure access restrictions, click **Catalogs > Protection > *SharePoint_Security* > Access Restrictions**. Use the **Allowed IP** list or **Banned IP** list to designate particular IP addresses or IP address ranges that should be handled differently:

- Allowed IP addresses are exempt from any limits on Concurrent Connections and Connection Rate.
- Banned IP addresses have their connection attempts rejected.