Pulse Secure Virtual Traffic Manager and Microsoft Exchange 2016

Deployment Guide

Contents

Preface

Welcome to the Pulse Secure Virtual Traffic Manager Solution Guide for load balancing and optimization of Microsoft Exchange 2016. Read this preface for an overview of the information provided in this guide and for contact information. This preface includes the following sections:

- About This Guide
- Contacting Pulse Secure

About This Guide

The Pulse Secure Virtual Traffic Manager Solution Guide describes how to configure Traffic Manager, to load balance and optimize Microsoft Exchange 2016 Mailbox servers.

This solution guide is designed to be used together with the following documentation:

- Pulse Secure Virtual Traffic Manager documentation

Audience

This guide is written for network administrators, Microsoft Exchange administrators, and developer-operations (DevOps) professionals familiar with administering and managing both Application Delivery Controllers (ADCs) and Microsoft Exchange.

You should also be familiar with:

- Microsoft Exchange network protocols including HTTP, SMTP, POP and IMAP
- Installing and configuring a virtual appliance in either a virtual VMWare, Hyper-V, or dedicated Linux environment

For more details on the Pulse Secure vADC product family, see: http://www.pulsesecure.net/vadc

Contacting Pulse Secure

This section describes how to contact departments within Pulse Secure.

Internet

You can learn about Pulse Secure products through the company Web site: http://www.pulsesecure.net/.

Technical Support

If you have problems installing, using, or replacing Pulse Secure products, contact Pulse Secure Support or your channel partner who provides support. To contact Pulse Secure Support, see https://www.pulsesecure.net/support/.

Professional Services

Pulse Secure Global Services has the expertise to help organizations build scalable and efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Pulse Secure Global Services delivers world- class professional services, technical support, and education services, enabling organizations to maximize their Pulse Secure investments, accelerate new technology deployments, and optimize the performance of networking infrastructures.

Chapter 1: Solution Overview

This chapter describes how Pulse Secure Virtual Traffic Manager provides advanced load balancing and application delivery controller features for Microsoft Exchange 2016, the factors you need to consider when designing your Traffic Manager deployment, and how and when to implement the most commonly used features.

This chapter includes the following sections:

- Virtual Traffic Manager Overview
- What's new in Microsoft Exchange 2016
- Why vTM to load balance and optimize Exchange 2016

Virtual Traffic Manager Overview

Pulse Secure Virtual Traffic Manager (vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public web sites and private applications. vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run on any physical, virtual, or cloud environment. With vADC products from Pulse Secure, organizations can:

- Make applications more reliable with local and global load balancing
- Scale application servers by up to 3x by offloading TCP and SSL connection overhead
- Accelerate applications by up to 4x by using web content optimization (WCO)
- Secure applications from the latest application attacks, including SQL injection, XSS, CSRF, and more
- Control applications effectively with built-in application intelligence and full-featured scripting engine

Virtual Traffic Manager offers much more than basic load balancing. It controls and optimizes end-user services by inspecting, transforming, prioritizing, and routing application traffic. The powerful TrafficScript® engine facilitates the implementation of traffic management policies that are unique to an application by allowing organizations to build custom functionality or to leverage existing features in Virtual Traffic Manager in a specialized way. With vTM, organizations can deliver:

Performance

Improve application performance for users by offloading encryption and compression from the web server by dynamic caching and reducing the number of TCP sessions on the application.

Reliability and scalability

Increase application reliability by load balancing traffic across web and application servers, balancing load across multiple data centers (private or public clouds), monitoring the response time of servers in real-time to decide the fastest way to deliver a service, protecting against traffic surges, and by managing the bandwidth and rate of requests used by different classes of traffic.

Advanced scripting and application intelligence

Manage application delivery more easily with fine-grained control of users and services using TrafficScript, an easy-to-use scripting language that can parse any user transaction, and take specific, real-time action based on user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, while operations teams use it to quickly respond to changing business requirements or problems within an application before developers can fix it.

Application acceleration

Dramatically accelerate web-based applications and websites in real-time with optional web content optimization (WCO) functionality. It dynamically groups activities for fewer long distance round trips, resamples and sprites images to reduce bandwidth, and minifies JavaScript and combines style sheets to give the best possible response time for loading a web page on any browser or device.

Application-layer security

Enhance application security by filtering out errors in web requests, and protecting against external threats, with the option of a comprehensive Layer-7 firewall to defend against deliberate attacks.

What's new in Microsoft Exchange 2016

Today, CPU horsepower is significantly less expensive and is no longer a constraining factor. With that constraint lifted, the primary design goal for Exchange 2016 is for simplicity of scale, hardware utilization, and failure isolation. With Exchange 2016, we reduced the number of server roles to two: the Mailbox and Edge Transport server roles.

The Mailbox server in Exchange 2016 includes all of the server components from the Exchange 2013 Mailbox and Client Access server roles:

- Client Access services provide authentication, limited redirection, and proxy services. Client Access services don't do any data rendering and offer all the usual client access protocols: HTTP, POP and IMAP, and SMTP.
- Mailbox services include all the traditional server components found in the Exchange 2013 Mailbox server role: the backend client access protocols, Transport service, Mailbox databases, and Unified Messaging. The Mailbox server handles all activity for the active mailboxes on that server.

The Edge Transport role is typically deployed in your perimeter network, outside your internal Active Directory forest, and is designed to minimize the attack surface of your Exchange deployment. By handling all Internet-facing mail flow, it also adds additional layers of message protection and security against viruses and spam, and can apply mail flow rules (also known as transport rules) to control message flow.

For a complete list of new features and changes in Exchange 2016, refer to the Microsoft TechNet links below:

- What's Discontinued in Exchange 2016
- Architectural changes in load balancing for Exchange Server 2016

Why vTM to load balance and optimize Exchange 2016

Pulse Secure Virtual Traffic Manager has significant advantages over other ADCs for load balancing and optimizing Microsoft Exchange 2016:

Application-Centric View

- Ability to deploy a separate ADC per application or tenant
- Ability to dynamically right-size the Pulse Secure Virtual deployment to fit the application needs
- Dynamic provisioning and scaling of ADC resources

Designed with Service Providers in Mind

- Designed as 64-bit software, that can be deployed in a VMWare or Hyper-V environment or as a dedicated software installation, instead of a physical appliance

- Multi-core packet processing for scalability
- Robust APIs for simple automated provisioning and management

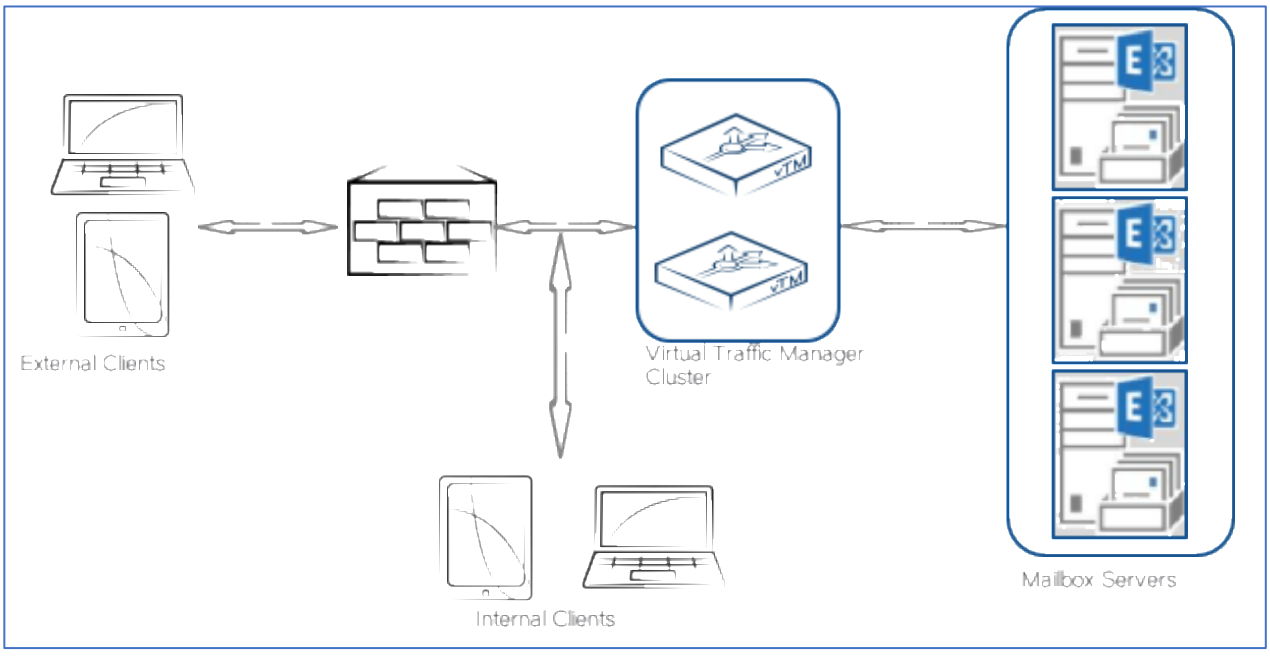
Designed for Services

- Global Load balancing, SSL offload, Caching, Service level management capabilities
- Application firewalling and web content optimization
- Robust and open APIs

Chapter 2: Microsoft Exchange 2016 Architecture

Pulse Secure Virtual Traffic Manager is a straightforward deployment to an existing network infrastructure with little to no changes required on the network. The Pulse Secure Virtual Traffic Manager can be deployed to provide support for both internal and external clients. DNS configuration is used to redirect traffic for internal and external clients to Pulse Secure Virtual Traffic Manager. Clustering of Pulse Secure vTMs can be used to provide high availability and load balancing to support a large amount of traffic and fault tolerance.

Figure 2-1 Microsoft Exchange Server



Like Exchange 2013, Exchange 2016 does not require session affinity. For a given protocol session, the Client Access services located on the Mailbox server maintain a 1:1 relationship with the Mailbox server hosting the user's data. In the event that the active database copy is moved to a different Mailbox server, sessions always end up at the Mailbox server hosting the active database copy.

If the client leverages the HTTP(s) protocol, then the protocol used between Mailbox servers is HTTP(s). If the protocol leveraged by the client is IMAP or POP, then the protocol used between the Mailbox servers is IMAP or POP.

However, there is a concern with this architectural change. Since session affinity is not used by the load balancer, this means that the load balancer has no knowledge of the target URL or request content. All the load balancer uses is layer 4 information, the IP address and the protocol/port. For this reason, if a specific service on the Mailbox server is down, traffic is still sent to the server due to the lack of health check on a particular service.

Exchange 2016 includes a built-in monitoring solution, known as Managed Availability. Managed Availability includes an offline responder. When the offline responder is invoked, the affected protocol (or server) is removed from service. To ensure that load balancers do not route traffic to a Mailbox server that Managed Availability has marked as offline, load balancer health probes must be configured to check <virtualdirectory>/healthcheck.htm. If the load balancer health probe receives a 200 status response, then the protocol is up; if the load balancer receives a different status code, then Managed Availability has marked that protocol instance down on the Mailbox server. As a result, the load balancer should also consider that end point down and remove the Mailbox server from the applicable load balancing pool.

Based on the possibility of doing a heatlh check specific to a service, Exchange 2016 HTTPS services can be load balanced using any one of the following deployment scenarios:

Deployment Type	Pros	Cons
Single Virtual Server – L4 (Optional and not covered in this guide)	Quick setup Consumes less resources on vTM	No health monitoring per Exchange HTTP service
Single Virtual Server - L7	Health monitoring per Exchange HTTP service Single external IP address and URL	Consumes more resources on vTM
Multiple Virtual Servers – L7	Isolated services with health monitoring	Uses more IP address space Complex configuration

Chapter 3: Deploying Pulse Secure Virtual Traffic Manager

This chapter describes the procedures for deploying Pulse Secure Virtual Traffic Manager for load balancing and optimizing Microsoft Exchange 2016 Mailbox Servers. It includes the following sections:

- Requirements
- Configuration steps for Single Virtual Server in L7 mode
- Configuration steps for Multiple Virtual Servers in L7 mode
- Configuration steps for IMAP3 and POP3
- Additional Optional Functionality on Pulse Secure Virtual Traffic Manager

Requirements

- Pulse Secure Virtual Traffic Manager (10.x)
- Microsoft Exchange 2016

The following are the prerequisites for deploying Exchange 2016 with Pulse Secure Virtual Traffic Manager:

Exchange 2016 Port Requirements

The following table describes the ports used by Exchange 2016.

MailBox Service Name	Protocol	TCP Port	Description
• Autodiscover service • Exchange ActiveSync • Exchange Web Services (EWS) • Offline address book (OAB) distribution • Outlook Anywhere (RPC over HTTP) • Outlook MAPI over HTTP • Outlook on the web	HTTPS	443	Encrypted web connections are used by clients and web services for the mentioned services
• Internet calendar publishing • Outlook on the web (redirect to 443/TCP) • Autodiscover (fallback when 443/TCP isn't available)	HTTP	80	Wherever possible encrypted web connections on 443 must be used for protection but some services must be configured to use unencrypted web connections on port 80 to the client access services on Mailbox servers
POP3 clients	POP3 / POP3s	110, 995	Post Office Protocol 3 is an email protocol that supports offline mail processing
IMAP4	IMAP4 / IMAP4s	143, 993	Interactive Mail Access Protocol is an email protocol that supports offline and online mail processing

Certificate Requirement

In Exchange 2016 Mailbox server, all communications are done via HTTPS. Data is encrypted using certificates. A client can be redirected to a different Mailbox server in a pool of servers that is different to the server that authenticated it originally. To avoid client to authenticate again against a different server and to ensure that data is decrypted correctly, use a certificate that is shared among the Mailbox servers and Pulse Secure Virtual Traffic Manager (vTM).

A single certificate using Subject Alternative Name (SAN) extension can be used to support all services on a Mailbox server. If separate certificates are used for different services, ensure that those certificates are imported into all other Mailbox servers and vTMs as appropriate.

Pulse Secure Virtual Traffic Manager Platform Support

Pulse Secure Virtual Traffic Manager is available on different platforms such as Linux, Solaris, Hyper-V, and VMWare; it can be installed as pure software or as a virtual appliance. The Pulse Secure Virtual Traffic Manager is available for download at http://www.pulsesecure.net/vadc/vtm.

Configuration Steps for Single Virtual Server in L7 mode

This approach uses a single IP address that is mapped to the FQDN of all the Exchange HTTP services and uses multiple Pools for each service. Using a TrafficScript, Traffic Manager directs the traffic to its appropriate Pool, and each pool can be monitored separately.

This section contains step by step instructions on configuring Traffic Manager for Single Virtual Server for all Exchange HTTP services with Multiple Pools:

Component	Procedure	Description
Virtual Traffic Manager (once)	Create Traffic IP Group for each Exchange HTTP Service	A single Traffic IP Group must be created for all Exchange services. For details, see “Create Traffic IP Groups”
Virtual Traffic Manager (repeat for each service)	Create Pool for each Exchange HTTP Service	Enter the hostname or IP address of the node along with the TCP/UDP port. For details, see “Create Pools”
	Select a Monitor for the Pool	Select a health monitor for the pool. For details, see “Create Monitors”
Virtual Traffic Manager (once)	Create Virtual Server for each Exchange HTTP Service	Create and associate the Virtual Server to the server pool of choice and the Traffic IP Group to listen on. For details, see “Create Virtual Server”
Virtual Traffic Manager (once)	SSL decryption	Configure SSL Decryption to enable SSL offloads. For details, see “SSL Decryption”
Virtual Traffic Manager (once)	Create and associate a Traffic Script that forwards the requests to appropriate pool with the virtual server	Configure Traffic Script to forward requests to relevant pools. For details, see “Create & associate Traffic Script”

Create a Traffic IP Groups

Create a Traffic IP Group (also known as a Virtual IP) on which the Virtual server will be listening on. To create a new Traffic IP Group:

1. Navigate to **Services->Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name:** A descriptive name for the Exchange HTTP Services (e.g. mail-lb.company.com)
   - **IP Addresses:** An IP Address that is mapped to FQDN of all the Exchange HTTP Services
3. Click **Create Traffic Group**.

Create Pools

For each of the identified Exchange HTTP Services, create a Pool using the steps below:

1. Navigate to **Services->Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name:** A descriptive name for the pool. (e.g. OWA Service)
   - **Nodes:** hostname:443 or ipaddress:443
   - **Monitor:** No Monitor (This will be covered in detail in later section)
3. Click on the **SSL Settings**.
4. Check the **Yes** button next to **ssl_encrypt**.
5. Click on **Update** button to apply changes.

Repeat steps 1 – 5 to create a Pool for each Exchange HTTP Service.

Create Monitors

The following sections detail the steps to create health monitors.

Note: Advanced external monitors can be written in any language of choice and be associated with the pool.

Create a Health Monitor that will monitor health of a Pool.

1. Navigate to **Catalogs->Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
7. Change **host_header** to the Service URL path (e.g., owa.company.com).
8. Change **Path:** to **/<Path>/healthcheck.htm** (e.g., /OWA/healthcheck.htm).
9. Change **status_regex** to **^200$**.
10. Change **body_regex** to **.*200 OK**.
11. Scroll down to **Apply Changes** and click the **Update** button.
12. Navigate to **Services->Pools** and select the pool that the monitor will be attached to.
13. Scroll down and click **Health Monitoring**.
14. Add the appropriate health monitor.

Repeat steps 1 – 14 to create a health monitor for each Exchange HTTP Service Pool. Refer to the table below for the path that should be used for each service.

Service Name	Path
Outlook Anywhere (OA)	/rpc/healthcheck.htm
Autodiscover	/Autodiscover/healthcheck.htm
Exchange Web Service (EWS)	/EWS/healthcheck.htm
Exchange Admin Center (EAC)	/ECP/healthcheck.htm
Outlook on the Web (OWA)	/OWA/healthcheck.htm
Exchange ActiveSync (EAS)	/Microsoft-Server-ActiveSync/healthcheck.htm
Offline Address Book (OAB)	/OAB/healthcheck.htm
MAPI	/mapi/healthcheck.htm

Create Virtual Server

Create a Virtual Server that will handle all the Exchange traffic. To create a new Virtual Server:

1. Navigate to **Services->Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name:** A descriptive name for the Virtual Server
   - **Protocol:** HTTP
   - **Port:** 443
   - **Default Traffic Pool:** Select any pool created in the previous section
3. Click on **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate Traffic IP Group that was created earlier.
5. Set **Enabled** to **Yes**.
6. Click on the **Update** button to apply changes.

SSL Decryption

In order to perform SSL decryption, import the SAN certificate and the private key used for all services.

1. Navigate to the **Catalogs->SSL->SSL Certificates** catalog.
2. Click on **Import Certificate** to import the appropriate certificate.

After importing the certificate, enable SSL Decryption on the Virtual Server created:

1. Navigate to **Services->Virtual Servers** and select the virtual server created for Exchange HTTP Services that will be performing SSL decryption.
2. Scroll down and click on **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in the previous step.
5. Scroll down to the bottom of the page and click **Update**.

Create and associate a Traffic Script that forwards the requests to appropriate pool with the virtual server

Since a single virtual server is used for all Exchange 2016 HTTP services, incoming traffic should be forwarded to an appropriate pool. This can be done via TrafficScript in Pulse Secure Virtual Traffic Manager. To create a traffic script that can accept variables, follow steps below:

1. Navigate to **System->Global Settings->Other Settings**.
2. Set **trafficscript!variable_pool_use** to **Yes**.
3. Scroll down to the bottom of the page and click the **Apply** button.
4. Navigate to **Catalogs->Rules**.
5. Create a new rule:
   - Name: A descriptive name for the Rule (e.g. Exchange 2016 Single Traffic IP)
   - User Traffic Script Language
6. Click on **Create Rule**.

7. Use the TrafficScript in Appendix for the syntax.
8. Click on the **Update** button.
9. Navigate to **Services->Virtual Servers** and select the virtual server created for Exchange HTTP Services that will be performing the TrafficScript created.
10. Scroll down and click on **Rules**.
11. Assign the TrafficScript to the Request Rules by clicking **Add Rule**.

Configuration Summary

By accessing the **Services->Config Summary** on the WebGUI, a complete snapshot of all the configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuration Steps for Multiple Virtual Servers in L7 mode

Deploying the Traffic Manager with multiple Virtual Servers requires provisioning an IP address for each virtual server created for every Exchange HTTP service. This approach provides health monitoring per HTTP service, and each virtual server can be managed independently from one another.

Component	Procedure	Description
Virtual Traffic Manager (repeat for each service)	Create Traffic IP Group for each Exchange HTTP Service	A Traffic IP Group must be created for each Exchange service. For details, see “Create Traffic IP Groups”
Virtual Traffic Manager (repeat for each service)	Create Pool for each Exchange HTTP Service	Enter the hostname or IP address of the node along with the TCP/UDP port For details, see “Create Pools”
	Select a Monitor for the Pool	Select a health monitor for the pool. For details, see “Create Monitors”
Virtual Traffic Manager (repeat for each service)	Create Virtual Server for each Exchange HTTP Service	Create and associate the Virtual Server to the server pool of choice and the Traffic IP Group to listen on. For details, see “Create Virtual Servers“
Virtual Traffic Manager (repeat for each service)	SSL decryption	Configure SSL Decryption to enable SSL offloads. For details, see “SSL Decryption”

Create Traffic IP Groups

Identify Exchange HTTP Services (as captured in the Exchange 2016 Port requirements section above) being offered by Mailbox servers, and create a Traffic IP Group for each service. Create a Traffic IP Group (also known as a Virtual IP) on which the Virtual Server will be listening. To create a new Traffic IP Group:

1. Navigate to **Services->Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name:** A descriptive name for the Traffic IP Group (e.g. owa.company.com)
   - **IP Addresses:** An IP Address that will be associated to FQDN of this service
3. Click on the **Create Traffic Group** button.

Repeat steps 1 – 3 for each Exchange Service that will be load balanced through Pulse Secure Virtual Traffic Manager.

Create Pools

For each of the identified Exchange HTTP Services, create a Pool using the steps below:

1. Navigate to **Services->Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name:** A descriptive name for the pool. (e.g. OWA Service)
   - **Nodes:** hostname:443 or ipaddress:443
   - **Monitor:** No Monitor (This will be covered in detail in later section)
3. Click on the **SSL Settings**.
4. Check the **Yes** button next to **ssl_encrypt**.
5. Click on **Update** button to apply changes.

Repeat steps 1 – 5 to create a Pool for each Exchange Service.

Create Monitors

The following sections detail the steps to create health monitors.

Note: Advanced external monitors can be written in any language of choice and be associated with the pool. Create a Health Monitor that will monitor health of a Pool.

1. Navigate to **Catalogs->Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
7. Change **host_header** to Service URL path (e.g., owa.company.com).
8. Change **Path:** to **/<Path>/healthcheck.htm** (e.g., /OWA/healthcheck.htm).
9. Change **status_regex** to **^200$**.
10. Change **body_regex** to **.*200 OK**.
11. Scroll down to **Apply Changes** and click the **Update** button.

12. Navigate to **Services->Pools** and select the pool that the monitor will be attached to.
13. Scroll down and click **Health Monitoring**.
14. Add the appropriate health monitor.

Repeat steps 1 – 14 to create a health monitor for each Exchange Service Pool. Refer to the table below for the path that should be used for each service.

Service Name	Path
Outlook Anywhere (OA)	/rpc/healthcheck.htm
Autodiscover	/Autodiscover/healthcheck.htm
Exchange Web Service (EWS)	/EWS/healthcheck.htm
Exchange Admin Center (EAC)	/ECP/healthcheck.htm
Outlook on the Web (OWA)	/OWA/healthcheck.htm
Exchange ActiveSync (EAS)	/Microsoft-Server-ActiveSync/healthcheck.htm
Offline Address Book (OAB)	/OAB/healthcheck.htm
MAPI	/mapi/healthcheck.htm

Create Virtual Servers

For each of the identified Exchange HTTP Services, create a Virtual Server using the steps below:

1. Navigate to **Services->Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name:** A descriptive name for the Virtual Server (e.g. owa.company.com)
   - **Protocol:** HTTP
   - **Port:** 443
   - **Default Traffic Pool:** Select the pool created for this service
3. Click on **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate Traffic IP Group that was created for the service.
5. Set **Enabled** to **Yes**.
6. Click on the **Update** button to apply changes.

Repeat steps 1 – 6 to create a Virtual Server for each Exchange Service.

SSL Decryption

In order to perform SSL decryption, import the SAN certificate and the private key used for each service created.

1. Navigate to **Catalogs->SSL->SSL Certificates** catalog.
2. Click on **Import Certificate** to import the appropriate certificate.

After importing the certificate, enable SSL decryption on the Virtual Server created:

1. Navigate to **Services->Virtual Servers** and select the virtual server created for the specific service that will be performing SSL decryption.
2. Scroll down and click on **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in the previous step.
5. Scroll down to the bottom of the page and click **Update**.

Repeat steps 1 – 5 for each Exchange Service.

Configuration Summary

By accessing the **Services->Config Summary** on the WebGUI, a complete snapshot of all the configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Configuration Steps for IMAP3 and POP3

IMAP4 and POP3 services on Exchange 2016 enable mail clients that support IMAP4 and POP3 protocols to access Exchange 2016 Mailbox servers running IMAP4 and POP3 services. By default, these services are disabled in Exchange 2016. To support these protocols, IMAP4 and POP3 services should be enabled.

For more information about how to manage and configure POP3 and IMAP4 in Exchange 2016, see POP3 and IMAP4 on Microsoft TechNet at https://technet.microsoft.com/en-us/library/jj657728(v=exchg.160).aspx

Component	Procedure	Description
Virtual Traffic Manager (once for each service)	Create Traffic IP Group for POP3 and IMAP4 Services	A Traffic IP Group must be created on which a Virtual Server listens. For details, see “Create Traffic IP Group”
Virtual Traffic Manager (once for each service)	Create Pool for POP3 and IMAP4 Services	A Pool needs to have a set of servers to load-balance. Enter the hostname or IP address of the node along with the TCP/UDP port. For details, see “Create Pools”
Virtual Traffic Manager (once for each service)	Create Virtual Server for POP3 and IMAP4 Services	Create and associate the Virtual Server to the server pool. For details, see “Create Virtual Servers“
Virtual Traffic Manager (once for each service)	SSL decryption for POP3 and IMAP4 Services	Configure SSL Decryption to enable SSL offloads. For details, see “SSL Decryption”

Create Traffic IP Group

Create a Traffic IP Group (also known as a Virtual IP) on which the Virtual Server will be listening. To create a new Traffic IP Group:

1. Navigate to **Services->Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Enter the following:
   - **Name:** A descriptive name for the POP3 and IMAP3 pool, assuming that POP3 and IMAP4 FQDN resolves to the same Traffic IP Group (e.g., pop.company.com)

- **IP Addresses:** An IP Address that will be associated to FQDN of the POP3 and IMAP4 service

3. Click the **Create Traffic Group** button.

Create Pools

A Pool has to be created for each service managed by the Traffic Manager. To create a new Pool:

1. Navigate to **Services->Pools** and scroll down to **Create a new Pool**.
2. Fill in the fields as follows:
   - **Pool Name:** A descriptive name for the pool.
   - **Nodes:** hostname:110 or ipaddress:110
   - **Monitor:** POP
3. Click on the **Update** button to apply changes.

Repeat steps 1-3 for create a new pool for IMAP4 using **port 143** for the **Nodes**.

For IMAP4, the health monitor should be a TCP transaction monitor. Follow the steps to create a new health monitor:

1. Navigate to **Catalogs -> Monitors -> Create New Monitor.** Type a name and select **TCP Transaction Monitor**.
2. Use the following values for parameters:
   - close_string: **logout\r\n**
   - delay: **10**
   - response_regex: *** OK.***
   - timeout: **10**
3. Navigate to **Services->Pools** and under **Health Monitoring**, select the created Monitor.

Create Virtual Servers

Create a Virtual Server that will handle all the traffic. To create a new Virtual Server:

1. Navigate to **Services->Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name:** A descriptive name for the Virtual Server
   - **Protocol:** POP3
   - **Port:** 995
   - **Default Traffic Pool:** Select the pool created in the previous section
3. Click on **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate Traffic IP Group that was created earlier
5. Set **Enabled** to **Yes**.
6. Click on the **Update** button to apply changes.

Repeat steps 1-6 to create a Virtual Server for IMAP4 using **Protocol: IMAP4** and **Port: 993**.

SSL Decryption

In order to perform SSL decryption, import the certificate with the appropriate SAN.

1. Navigate to **Catalogs->SSL->SSL Certificates** catalog.
2. Click on **Import Certificate** to import the appropriate certificate.

After importing the certificate, enable SSL Decryption on the Virtual Server created:

1. Navigate to **Services->Virtual Servers** and select the virtual server created for POP3 that will be performing SSL Decryption.
2. Scroll down and click on **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in the previous step.
5. Scroll down to the bottom of the page and click **Update**.

Repeat steps 1-5 to enable SSL decryption on the Virtual Server for IMAP4.

Configuration Summary

By accessing the ***Services->Config Summary*** on the WebGUI, a complete snapshot of all the configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Virtual Servers ▽	Rules	Pools	Nodes
imap.company.com **pop.company.com**:993	*Use default pool*	**Exchange 2013 IMAP4 Service**	company-cas1:143 company-cas2:143
pop.company.com **pop.company.com**:995	*Use default pool*	**Exchange 2013 POP3 Service**	company-cas1:110 company-cas2:110

Additional Optional Functionality on Pulse Secure Virtual Traffic Manager

Pulse Secure Virtual Traffic Manager has additional capabilities beyond a legacy load balancer to enhance the performance and manageability of your Microsoft Exchange 2016 environment. Here are some common capabilities and best practices for deploying Pulse Secure Virtual Traffic Manager to enhance your Microsoft Exchange 2016 deployment:

Service Level Monitoring

Service Level Monitoring continually checks the responses of your Mailbox servers and can send alerts should these fall below an expected threshold of performance. In addition to sending alerts, TrafficScript can be used to remove the service or server from the pool until the performance issue has been fixed. TrafficScript can also be used to reprioritize traffic, and even reallocate bandwidth. This capability increases the availability and service level of Microsoft Exchange.

Configuring Traffic Manager for Service Level Monitoring of Exchange 2016 is outside the scope of this document. For more information, please contact Pulse Secure.

Global Load Balancing

Global Load Balancing enables Client Access Servers to be distributed across multiple locations, for either business continuity/disaster recovery or for locating the servers geographically closer to end users. This enables seamless failover if a datacenter has an outage, and greater performance for users distributed geographically.

Configuring Traffic Manager for Global Load Balancing is outside the scope of this document. For more information, please contact Pulse Secure.

Digital Certificates and SSL

All communication between client and server is done through SSL. Pulse Secure Virtual Traffic Manager can use certificates to decrypt incoming services such as POP3 and IMAP4. In addition, it provides SSL offloading for earlier versions of Exchange like Exchange 2010. To provide SSL decryption and offloading, the certificates should be imported into Pulse Secure Virtual Traffic Manager.

Microsoft best practices recommend the use of trusted third-party SAN certificates that can represent multiple domain names, and Pulse Secure recommends you follow these suggestions and best practices provided by Microsoft on TechNet:

https://technet.microsoft.com/en-us/library/dd351044(v=exchg.160).aspx

Redirecting OWA HTTP requests to SSL

Pulse Secure Virtual Traffic Manager can easily be configured to help clients accessing OWA through non-encrypted port 80 to be redirected automatically to connect on SSL.

This section contains step by step instructions for configuring Traffic Manager for Redirecting all HTTP requests to SSL:

- Create a Virtual Server with Traffic Pool set to Discard
- Create a Traffic Script to redirect to proper SSL URL
- Associate the redirect TrafficScript to the Virtual Server

Create a Virtual Server with Traffic Pool Set to Discard

Create a Virtual server that will handle all the OWA traffic. To create a new Virtual Server

1. Enter the following:
   - **Virtual Server Name:** A descriptive name for the Virtual Server
   - **Protocol:** HTTP
   - **Port:** 80
   - **Default Traffic Pool:** discard
2. Click on **Create Virtual Server**.
3. In the next screen, set **Enabled:** to **Yes**.
4. Click on the **Update** button to apply changes.

Create a Traffic Script to redirect to proper SSL URL

1. Navigate to **Catalogs->Rules**.
2. Create new rule:
   - Name: A descriptive name for the Rule (e.g., OWA_Redirect_SSL)
   - User Traffic Script Language
3. Click on **Create Rule**.
4. Use the TrafficScript in Appendix for the syntax.
5. Click on the **Update** button.
6. Navigate to **Services->Virtual Servers** and select the virtual server that will be performing the TrafficScript created.

7. Scroll down and click on **Rules**.
8. Assign the TrafficScript to the Request Rules by clicking **Add Rule**.

Configure Clustering for Pulse Secure Virtual Traffic Manager

To provide high availability and fault tolerance for Pulse Secure Virtual Traffic Manager, they can be joined into a cluster and configured to load balance or act as active-passive mode for fault tolerance.

Use the following steps to join a Pulse Secure Virtual Traffic Manager to an existing cluster:

1. Navigate to **System->Traffic Managers**.
2. Scroll down to **Add or Remove Traffic Managers** and click on **Join a Cluster**.
3. Click **Next** on **Getting Started**.
4. Select the cluster to join and click **Next**.
5. Check the certificate used for the cluster, and provide Username and Password for the cluster, click **Next** to continue.
6. Select **Yes, and allow it to host Traffic IPs immediately** and click **Next**.
7. In the **Summary** page, click **Finish** to join the vTM to the cluster.

Chapter 4: Common Troubleshooting Tips

This chapter describes tips for troubleshooting common deployment issues.

Uploading certificates to Traffic Manager

When uploading a certificate to Traffic Manager, these must be in PEM format. For your certificates are not in PEM format, there are tools available to convert CER (without key) and PFX (with key) formats to PEM format, such as OpenSSL. To upload a certificate used by an Exchange server, export the certificate once with private key and once without private key. Use the following commands to convert the certificate to PEM format.

Convert a DER file (.crt .cer .der) to PEM

openssl x509 -inform der -in <certificate filename>.cer -out certificate.pem

Convert a PKCS#12 file (.pfx .p12) containing a private key and certificates to PEM

openssl pkcs12 -in <certificate key filename>.pfx -out certificatekey.pem -nodes

Chapter 5: Conclusion

This document discusses how to configure Traffic Manager to optimize the deployment of Microsoft Exchange 2016 application. Traffic Manager is able to make intelligent load balancing decisions and improve the performance, security, reliability and integrity of the traffic in this environment.

Appendix

Traffic Script code to configure Pulse Secure Virtual Traffic Manager for a single Virtual Server with multiple Pools

The Traffic Script code below is used to direct incoming traffic to its corresponding Pool.

```
#// TS Rule for Exchange 2016 for a Single VS with Multiple Pools
# Please declare the names of the pools you have configured, and ensure
# that the trafficscript!variable_pool_use Global setting is set to 'yes'

$owa_pool = "Exchange 2016 OWA";
$autodiscover_pool = "Exchange 2016 Autodiscover";
$ecp_pool = "Exchange 2016 ECP";
$ews_pool = "Exchange 2016 EWS";
$eas_pool = "Exchange 2016 EAS";
$oab_pool = "Exchange 2016 OAB";
$oa_pool = "Exchange 2016 OA";
$debug = 0; // Change value to 1 if debug needed

$path = http.getPath();
$pool = "";

#Exchange Autodiscover Pool
if( string.startsWithI( $path, "/autodiscover" ) ) {
    $pool = $autodiscover_pool;
    if ($debug > 0) { log.info("Auto Discover Pool Selected");}
}
#Exchange Control Panel Pool
else if( string.startsWithI( $path, "/ecp" ) ) {
    $pool = $ecp_pool;
    if ($debug > 0) { log.info(" Exchange Control Panel Pool Selected");}
}
# Exchange Web Services Pool
else if( string.startsWithI( $path, "/ews" ) ) {
    $pool = $ews_pool;
    if ($debug > 0) { log.info("Exchange Web Services Pool Selected");}
}
```

```
# Exchange Active Sync Pool
else if( $path == "/Microsoft-Server-ActiveSync" ) {
    $pool = $eas_pool;
    if ($debug > 0) { log.info("Exchange Active Sync Pool Selected");}
}
#Exchange Offline Address Book Pool
else if( string.startsWithI( $path, "/oab" ) ) {
    $pool = $oab_pool;
    if ($debug > 0) { log.info("Offline Address Book Pool Selected");}
}
#Exchange Outlook Anywhere Pool
else if( $path == "/rpc/rpcproxy.dll" ) {
    $pool = $oa_pool;
    if ($debug > 0) { log.info("Outlook Anywhere Pool Selected");}
}
#Exchange Outlook Web Access Pool
else {
    $pool = $owa_pool;
    if ($debug > 0) { log.info("Outlook Web Access Pool Selected");}
}

pool.select ( $pool );
```

Traffic Script code to redirect all HTTP requests to HTTPS

The Traffic Script code below is used to redirect OWA HTTP requests to HTTPS. Similar script can be written for other services.

```
#// TS Rule for redirecting HTTP requests to HTTPS
# Exchange 2016 OWA Redirect SSL
# Redirect to OWA URL if user tried default website
$debug = 0; // Change value to 1 if debug needed

$hostheader = http.getHostHeader();
If (http.getPath() == “/”)
{
   http.redirect(https://.$hostheader.”/owa”);
      if ($debug > 0) { log.info("Redirected to OWA URL");}
}
```