DEPLOYMENT GUIDE

Brocade Virtual Traffic Manager and Microsoft Skype for Business 2015 Deployment Guide

53-1004187-02
28 March 2017

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

Contents

Preface

About This Guide

The *Brocade Virtual Traffic Manager and Microsoft Skype for Business 2015 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft Skype for Business 2015. This deployment guide includes information relevant to the following products: Brocade Virtual Traffic Manager and Microsoft Skype for Business 2015.

For more details on the Brocade vADC product family, see http://www.brocade.com/vADC.

Audience

This guide is written for network administrators, Microsoft Skype for Business administrators, and developer operations (DevOps) professionals who are familiar with administering and managing both application delivery controllers (ADCs) and Microsoft Skype for Business. You should also be familiar with:

- Microsoft Skype for Business 2015 port requirements for both front-end and edge pools
- Microsoft Skype for Business 2015 load-balancing requirements for both front-end and edge pools
- Installing and configuring a virtual appliance in a VMware, Microsoft Hyper-V, or dedicated Linux environment

About Brocade

Brocade® (NASDAQ: BRCD) networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings (www.brocade.com).

Contacting Brocade

This section describes how to contact departments within Brocade.

Internet

You can learn about Brocade products through the company website: http://www.brocade.com.

Technical Support

If you have problems installing, using, or replacing Brocade products, contact Brocade Support or your channel partner who provides support. To contact Brocade Support, see http://www.brocade.com/en/support.html.

Professional Services

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

Document History

Date	Part Number	Description
January 2016	53-1004187-01	Initial release.
March 2017	53-1004187-02	Added vWAF content.

Solution Overview

This chapter describes how Brocade Virtual Traffic Manager provides advanced load-balancing and application delivery controller (ADC) features for Microsoft Skype for Business 2015, the factors to consider when designing your Virtual Traffic Manager deployment, and how and when to implement the most commonly used features.

Brocade Virtual Traffic Manager

Brocade Virtual Traffic Manager (Brocade vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public websites and private applications. Brocade vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run in any physical, virtual, or cloud environment. With vADC products from Brocade, 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, and CSRF.
- Control applications effectively with built-in application intelligence and a full-featured scripting engine.

Brocade 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 leverage existing features in Brocade vTM in a specialized way. With vTM, organizations can deliver the following:

- **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 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 the user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, whereas operations teams use it to quickly respond to changing business requirements or problems within an application before developers can fix them.
- **Application Acceleration**—Dramatically accelerate web-based applications and websites in real time with optional web content optimization (WCO) functionality. WCO dynamically groups activities for fewer long-distance round trips, resamples and sprites images to reduce bandwidth, and minifies and compresses 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.

Why Brocade Virtual Traffic Manager in Microsoft Skype for Business 2015

Brocade Virtual Traffic Manager has significant advantages over other ADCs for load-balancing and optimizing Microsoft Skype for Business 2015.

Application-Centric View

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

Designed with Service Providers in Mind

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

Designed for Services

- Global load balancing, SSL offloading, caching, service-level management capabilities
- Application firewalling and web content optimization
- Robust and open APIs

What’s New in Microsoft Skype for Business 2015

There are many new features and significant enhancements introduced in Microsoft Skype for Business 2015. The following list of notable changes is relevant to Microsoft Skype for Business 2015.

Enhanced Front-End Architecture

The Enterprise Edition front-end pool has shifted to a distributed systems architecture; real-time data is now stored on the front-end pool. One front-end server acts as the master for each user’s information, and two other front-end servers serve as replicas. When the master front-end server goes down, one of the replicas is automatically promoted to master. It is still possible to use only two front-end servers, but Microsoft recommends including at least three Enterprise Edition front-end servers in a front-end pool. This deployment guide takes into consideration the new recommendation from Microsoft.

Improved Front-End Server Patching and Upgrade Process

Skype for Business Server introduces two new cmdlets that help make upgrading or patching front-end servers much easier than in previous versions of Skype for Business Server. When you need to apply a patch or perform any other maintenance to a front-end server, simply type **Invoke-CsComputerFailOver** and specify that server’s name. Skype for Business Server temporarily moves that server’s workload to the other servers in the pool. You can then perform the maintenance and then use the **Invoke-CsComputerFailback** cmdlet to bring that server back into service. If you need to patch each server in a pool, simply follow this procedure for each server, one at a time. These new cmdlets enable you to patch servers much more quickly than in previous versions, with more reliability and with a simpler workflow.

Improved Front-End Pool Cold Start Capability

Skype for Business Server introduces a new cmdlet that simplifies and improves the process of cold-starting an entire front-end pool. When you use the new **Start-CsPool** cmdlet, it checks prerequisites for all front-end servers in the pool and then attempts to start each server. If it encounters problems, it diagnoses them and alerts you with details and workarounds. In some cases, it enables you to start the pool even if some individual servers are unable to start.

SQL Server AlwaysOn Support for On-Premises Servers

Skype for Business Server 2015 adds support for both SQL Server AlwaysOn Availability Groups and SQL Server AlwaysOn Failover Cluster Instances. In addition to these features, Skype for Business Server continues support for database mirroring and SQL Server clustering, as in past versions of Skype for Business Server.

SQL Server AlwaysOn Availability Groups is a high availability and disaster recovery solution in SQL Server 2012 and SQL Server 2014 that provides an alternative to database mirroring. An availability group supports a failover environment for a discrete set of databases (known as availability databases) that fail over together. An availability group supports a set of read-write primary databases and one to four sets of corresponding secondary databases. Optionally, secondary databases can be made available for read-only access and for some backup operations.

For more information, see the *Plan for high availability and disaster recovery in Skype for Business Server 2015*.

Multifactor Authentication

Multifactor authentication is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions; for example, requiring a user name and password, as well as a certificate. Skype for Business Server 2015 continues to build on the multifactor authentication features available in the Skype for Business Server 2013 cumulative updates. The significant changes in multifactor authentication are:

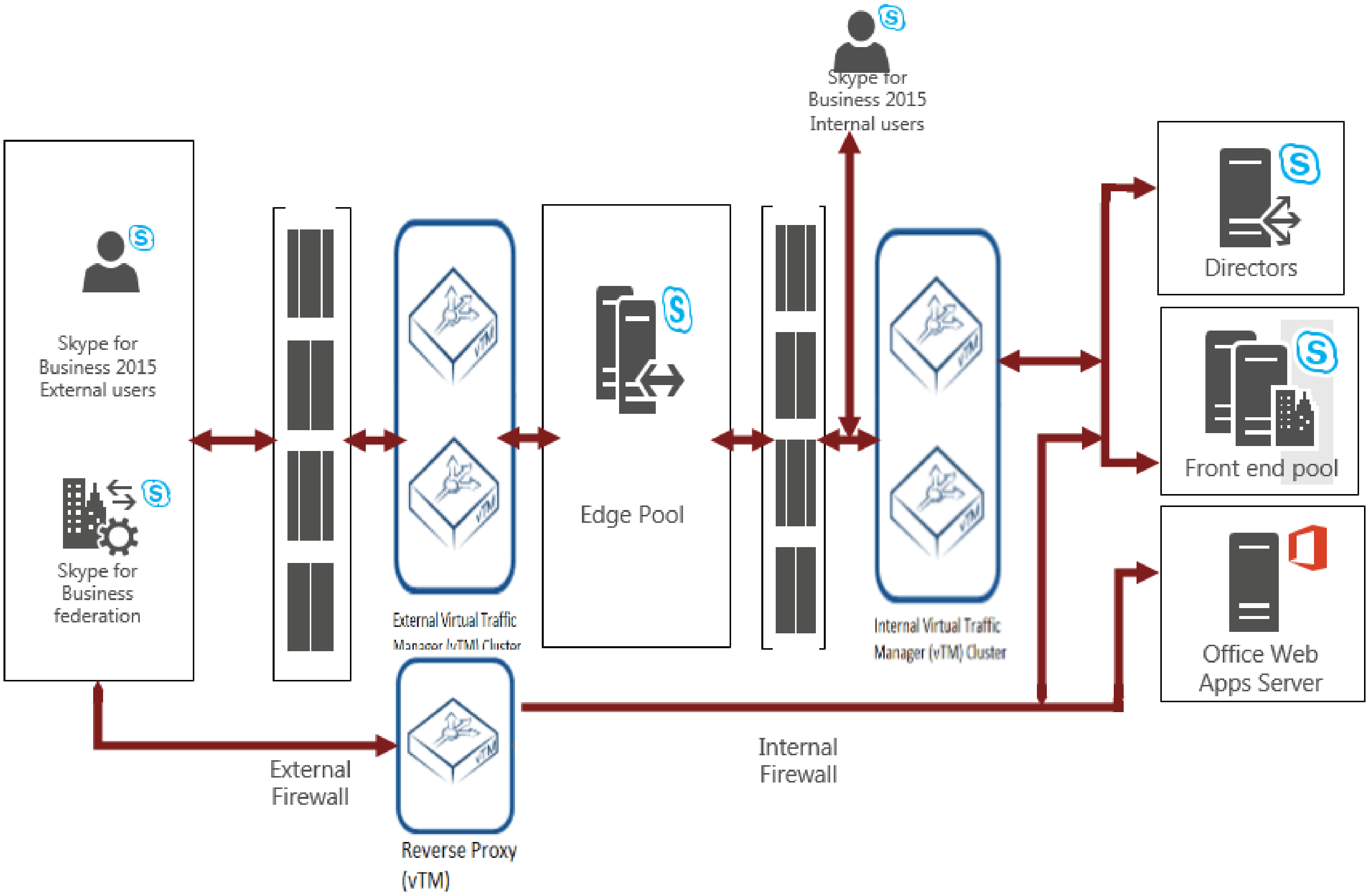
- Use of the Office 2013 SP1 Active Directory Authentication Library for integration with Exchange and SharePoint.
- Support for the multifactor authentication feature in the Skype for Business Web App client.
- With Skype for Business multifactor authentication, it is now possible to provide different authentication options based on geography.

For a complete list of changes, refer to *What's new in Skype for Business Server 2015*.

Microsoft Skype for Business 2015 Architecture

This section describes the recommended deployment topology for the Virtual Traffic Manager.

FIGURE 1 Recommended Topology



The recommended topology consists of two sets of Virtual Traffic Managers: one managing the external interface of the Skype for Business edge pool and the other managing the internal interface of the Skype for Business edge pool, the Skype for Business front-end pool, the optional Skype for Business director pool, and one other Virtual Traffic Manager acting as a reverse proxy. In this topology, it is important to note that the Skype for Business edge pool is in a perimeter network.

The main advantage of this deployment topology is that it improves security via the perimeter network. The perimeter network isolates the Skype for Business edge pools, which handle potentially dangerous traffic from the Internet.

Deploying Brocade Virtual Traffic Manager and Microsoft Skype for Business 2015

This chapter describes the procedures for deploying Brocade Virtual Traffic Manager for load-balancing and optimizing Microsoft Skype for Business 2015 servers.

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft Skype for Business 2015 Server
- IP address information for all Skype for Business hosts and VIPs

Internal Virtual Traffic Manager Configuration

The following sections highlight the IP groups, pools, and VIPs that need to be created on the internal pair of clustered Virtual Traffic Managers.

General Internal Virtual Traffic Manager Configuration

First we must perform some general configuration to leverage during the configuration. Let's start with the connection monitor. Two different types of health monitors must be created for Skype for Business. The following sections detail the steps to create these health monitors.

Creating Monitors

Creating a TCP Connect Monitor

The basic TCP Connect monitor is used by most Skype for Business services.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Enter a name for the new monitor in the **Name** field. Set **Type** to **TCP Connect Monitor** and **Scope** to **Node**.
4. Click **Create Monitor**.

Creating an HTTP Monitor

The HTTP monitor is used for port 8080 on the Skype for Business front-end pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Enter a name for the new monitor in **Name**. Set **Type** to **HTTP** and **Scope** to **Node**.
4. Click **Create Monitor**.
5. In the subsequent configuration page, scroll down and change the **path** to **/Autodiscover/AutodiscoverService.svc/root**.
6. Change **body_regex** to **.***.

Creating an IP-Based Persistence Class

A persistence class should be created for each desired persistence type and subnet. If you try to apply the same persistence class to different nodes on different subnets, an error occurs.

1. Navigate to **Catalogs** > **Persistence**.
2. Scroll down and create a new session persistence class.
3. Enter a name in the **Name** field for the new persistence class (ideally include type and subnet, e.g., IP Based Persistence - 10.255.74.x).
4. Click **Create Class**.
5. Scroll down to **Basic Settings**.
6. Set the type to **IP Based Persistence**.
7. Click **Update**.

Front-End Service Configuration

Each element that must be created for the front-end pool is detailed in the following table.

Component	Procedure	Description
Internal Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created to front the Skype for Business front-end pool. This includes the internal VIP for the front-end pool.
Internal Virtual Traffic Manager (repeat for each row in the Front-End Pool Table of Services on page 18)	Creating a Pool	A pool must be created per port, 16 pools in total. The IP address of each individual Skype for Business front-end server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Configure IP-based persistence on the pool.
	Configuring the TCP Connect Health Monitor	Configure the TCP connect health monitor for the pool.
	Creating a Virtual Server	A virtual server must be created per port based on the Skype for Business front-end pool table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes).	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

NOTE

If retaining Lync 2010 servers and using port 8080, configure transparent session affinity instead of IP-based session persistence.

Traffic IP Groups Needed

For Skype for Business 2015, up to six unique traffic IP groups must be created, namely:

- Front-End Pool
- Director Pool
- Edge Pool: Internal Interface
- Edge Pool: External Interface
- Edge Pool: A/V Service
- Edge Pool: Web Conferencing Service

Creating a Traffic IP Group for the Front-End Pool

Create a traffic IP group (also known as a virtual IP) for the front-end pool for each pool managed by the Virtual Traffic Manager. Per the previous table, start by creating the 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., sfb-fe-pool.company.com for the front-end pool)
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business Front-End Pool

Next create the front-end pool. The front-end pool manages many Skype for Business services and, as a result, uses many ports. The Front-End Pool Table of Services on page 18 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. The port is listed in the first column of the Front-End Pool Table of Services on page 18. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).

3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external access edge pools, edge external Web Conferencing services pools, and the edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   The following table contains a list of the Skype for Business services on the front-end pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (16 pools in total).

Front-End Pool Table of Services

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
80	HTTP	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) Only used when port 443 is not used
135	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Required for Address Book
443	SSL (HTTPS)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Communication with web farm
444	SSL (HTTPS)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Communication with Focus
448	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using Call Admission Control
5061	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	SIP/TLS
5067	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using a collocated or standalone Mediation Pool
5068	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using a collocated or standalone Mediation Pool
5070	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using a collocated or standalone Mediation Pool
5071	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Response Group Application
5072	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using Microsoft Skype for Business 2015 Attendant
5073	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) If using the Skype for Business Server Conferencing Announcement service
5075	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Call Park application

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
5076	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Audio Test service
5080	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Call Admission Control for A/V edge TURN traffic
8080	HTTP	Least Connections	IP-Based Persistence or Transparent Session Affinity (if deployment has Lync 2010 servers)	HTTP Monitor	No	(Optional) Used by web components for external access. Requires configuring SSL decryption and encryption if using transparent session affinity

Creating the Front-End Pool Virtual Servers

Each pool must be associated with a virtual server. Up to 16 virtual servers (one to match each pool created in the previous section). Create a virtual server using the following steps.

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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

About the Skype for Business Edge Pool

The Skype for Business edge pool allows users outside the corporate firewall to securely access Skype for Business without having to go through a VPN. The Skype for Business edge pool has two sets of interfaces: an external interface to communicate with external users and an internal interface to communicate with the Skype for Business front-end pool.

In this topology, there are two sets of Virtual Traffic Manager clusters, one managing the external interface of the Skype for Business edge pool and the other managing the internal interface of the Skype for Business edge pool along with the Skype for Business front-edge pool and optional Skype for Business director pool. An alternative deployment is to have a single cluster that manages all traffic.

Skype for Business Edge Internal Interface Service Configuration

The Skype for Business edge internal interface is the interface of the Skype for Business edge server that is inside the firewall. The configuration for the internal interface of the Skype for Business edge pool is done on the internal Virtual Traffic Manager. The Skype for Business Edge Internal Interface Service Table on page 21 is used in this section.

The following elements are needed to create the edge internal interface service configuration.

Component	Procedure	Description
Internal Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created for the internal interface of the Skype for Business edge pool.
Internal Virtual Traffic Manager (repeat for each row in the Skype for Business Edge Internal Interface Service Table on page 21)	Creating a Pool	A pool must be created per port. The IP address for the internal interface on each individual Skype for Business edge server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Create an IP-based persistence class for the pool.
	Configuring the TCP Connect Health Monitor	Configure the TCP connect health monitor for the pool.
	Creating a Virtual Server	A virtual server must be created per port in the Skype for Business edge pool internal interface table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

Creating a Traffic IP Group for the Edge Internal Interface Pool

Create a traffic IP group for the edge internal interface pool (also known as the virtual IP) for each pool managed by the Virtual Traffic Manager. Per the previous table, start by creating the 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., sfb-EII-pool.company.com for the edge internal interface pool)
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business Edge Internal Interface Pools

Next create the edge internal interface pools. These pools manage many Skype for Business services and, as a result, use many ports. The Skype for Business Edge Internal Interface Service Table on page 21 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. The port is listed in the first column of the Skype for Business Edge Internal Interface Service Table on page 21. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).

3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table, and click **Update**.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external access edge pools, edge external Web Conferencing services pools, and the edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   If you need to create additional persistence classes based on the note above, perform the following steps:

   1. Select **Catalogs** > **Persistence**.
   2. Scroll down and create a new session persistence class.
   3. Set the type according to the entry in the configuration table.

Attaching the Session Persistence Class to a Pool

1. Navigate to **Services** > **Pools**, and select the pool that the monitor will be attached to.
2. Scroll down, and click **Session Persistence.**
3. Choose the appropriate session persistence class.

Skype for Business Edge Internal Interface Service Table

The following table contains a list of the Skype for Business services on the internal interface of the edge pool along with the Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (six pools in total).

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
443	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Alternate media transfer port
3478	UDP	Least Connections	IP-Based Persistence	None	No	Preferred media transfer port
4443	Generic Client First	Least Connections	None	TCP Connect Monitor	No	Automatic topology replication
5061	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	SIP/TLS
5062	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	A/V Authentication service (SIP/TLS)
8057	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Web conferencing traffic

NOTE
There is no entry for the new XMPP port for the Skype for Business edge internal interface. Only the XMPP proxy is available for load balancing in the Virtual Traffic Manager (see https://technet.microsoft.com/en-us/library/gg615011.aspx).

External Virtual Traffic Manager Configuration

The following sections highlight the IP groups, pools, and VIPs that must be created on the external pair of clustered Virtual Traffic Managers.

General External Virtual Traffic Manager Configuration

We need to create the same two health monitors that were created on the internal cluster. The following sections detail the steps to create these health monitors.

Creating Monitors

Creating a TCP Connect Monitor

The basic TCP Connect monitor is used by most Skype for Business services.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Enter a name for the new monitor in the **Name** field. Set **Type** to **TCP Connect Monitor** and **Scope** to **Node**.
4. Click **Create Monitor**.

Creating an HTTPS Monitor

The HTTPS monitor is used if a reverse proxy is configured.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Enter a name for the new monitor in **Name**. Set **Type** to **HTTP** and **Scope** to **Node**.
4. Click **Create Monitor**.
5. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
6. Change the path to **/groupexpansion/service.svc**.
7. Change **body_regex** to **.***.

Creating Persistence Classes

Creating an IP-Based Persistence Class

A persistence class should be created for each desired persistence type and subnet. If you try to apply the same persistence class to different nodes on different subnets, an error occurs.

1. Navigate to **Catalogs** > **Persistence**.
2. Scroll down and create a new session persistence class.
3. Enter a name in the **Name** field for the new persistence class (ideally include type and subnet, e.g., IP Based Persistence - 10.255.74.x).
4. Click **Create Class**.
5. Scroll down to **Basic Settings**.

6. Set the type to **IP Based Persistence**.
7. Click **Update**.

Creating a Transparent Session Affinity Persistence Class

A transparent session affinity persistence class must be created if deploying and retaining Lync Server 2010 servers. If retaining Lync 2010 servers and using port 8080, configure transparent session affinity instead of IP-based session persistence.

1. Navigate to **Catalogs** > **Persistence**.
2. Scroll down and create a new session persistence class.
3. Enter a name in the **Name** field for the new persistence class (ideally include type and subnet, e.g., Transparent Session Affinity - 10.255.74.x).
4. Click **Create Class**.
5. Scroll down to **Basic Settings**.
6. Set the type to **Transparent Session Affinity**.
7. Click **Update**.

Reverse Proxy Service Configuration

If using a dual firewall DMZ deployment, an additional port must be added to the Virtual Traffic Manager. The port belongs to the director pool if that is configured; otherwise, the port belongs to the front-end pool. The Skype for Business Reverse Proxy Service Configuration Table on page 25 is used in this section.

Each element that must be created for the edge internal interface service configuration follows.

Component	Procedure	Description
Internal Virtual Traffic Manager (repeat for each row in the Skype for Business Reverse Proxy Service Configuration Table on page 25)	Creating a Pool	A pool must be created per port. The IP address of each individual Skype for Business director server (if used) or Skype for Business front-end server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence or Transparent Session Affinity on the Pool	If retaining Lync Server 2010 servers, configure transparent session affinity on the pool; otherwise, configure IP-based session persistence.
	Configuring the HTTP Health Monitor	Configure an HTTP health monitor for the pool.
	Creating a Virtual Server	A virtual server must be created per port based on the Skype for Business reverse proxy table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

NOTE
For Skype for Business Mobility in Skype for Business Server 2015, the mobility services use the reverse proxy and published services that are deployed on the front-end servers. No changes are required to the edge servers. Outbound SIP/TCP/5061 is needed from the server that runs the Skype for Business Server Access Edge service.

NOTE
On the reverse proxy publishing rule for port 4443, set **Forward Host Header** to **True** on the Virtual Traffic Manager. This will ensure that the original URL is forwarded.

Creating a Traffic IP Group for the Reverse Proxy Service Pool

Create a traffic IP group for the reverse proxy service pool (also known as the virtual IP) for each pool managed by the Virtual Traffic Manager.

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., sfb-EII-pool.company.com for the reverse proxy service pool)
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business Reverse Proxy Service Pools

Next create the reverse proxy service pools. These pools manage many Skype for Business services and, as a result, use many ports. The Skype for Business Reverse Proxy Service Configuration Table on page 25 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. The port is listed in the first column of the Skype for Business Reverse Proxy Service Configuration Table on page 25. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).
3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table, and click **Update**.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external Access Edge pools, edge external Web Conferencing services pools, and edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   If you need to create additional persistence classes based on the note above, perform the following steps:

   1. Select **Catalogs** > **Persistence**.
   2. Scroll down and create a new session persistence class.
   3. Set the type according to the entry in the configuration table.

Attaching the Session Persistence Class to a Pool

1. Navigate to **Services** > **Pools**, and select the pool that the monitor will be attached to.
2. Scroll down, click **Session Persistence.**
3. Choose the appropriate session persistence class.

   The following table contains a list of the Skype for Business services on the reverse proxy service pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (six pools in total).

Skype for Business Reverse Proxy Service Configuration Table

The following table contains a list of additional Skype for Business services to be configured along with the Virtual Traffic Manager settings if a reverse proxy is used.

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
4443	HTTP	Least Connections	IP-Based Persistence or Transparent Session Affinity (if deploying retaining Lync Server 2010 servers)	HTTPS Monitor	No	Traffic from reverse proxy requires configuring SSL decryption and encryption if using transparent session affinity.

Creating the Reverse Proxy Service Virtual Servers

Each pool must be associated with a virtual server: one virtual server to match each pool created in the previous section. 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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

About Skype for Business Edge Pool External Interface (Access Edge)

The Skype for Business edge pool allows users outside the corporate firewall to securely access Skype for Business without having to go through a VPN. The Skype for Business edge pool has two sets of interfaces: an external interface to communicate with external users and an internal interface to communicate with the front-end pool.

In this topology, there are two sets of Virtual Traffic Manager clusters, one managing the external interface of the Skype for Business edge pool and another managing the internal interface of the Skype for Business edge pool along with the Skype for Business front-edge pool and optional Skype for Business director pool. An alternative deployment is to have a single cluster that manages all traffic.

> NOTE
> The Skype for Business Server 2015 edge external interface requires three public IP address for vTM traffic IP addresses (a one-time requirement that does not increment as more edge servers are added to the pool), plus three public IP addresses *per* edge server in the pool. For more information, see Choosing a topology in the Skype for Business 2015 documentation on Microsoft TechNet . If the required number of public IP addresses cannot be secured, DNS load balancing must be used instead, because it supports NAT.

Skype for Business Edge Pool External Interface (Access Edge) Service Configuration

The Skype for Business edge pool external interface is the interface of the Skype for Business edge server that is outside the firewall. The following table contains a list of the Skype for Business services on the external interface of the edge pool along with Virtual Traffic Manager settings. A new port, XMPP, is used to allow communication with XMPP federated partners.

The Skype for Business Edge External Interface (Access Edge) Table on page 28 is used in this section.

Component	Procedure	Description
External Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created for the external interface of the Skype for Business edge pool.
External Virtual Traffic Manager (repeat for each row in the Skype for Business Edge External Interface (Access Edge) Table on page 28)	Creating a Pool	A pool must be created per port. The IP address for the external interface on each individual Skype for Business edge server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Create an IP-based persistence class for the pool.
	Configuring the TCP Connect Health Monitor	Create a TCP connect health monitor.
	Creating a Virtual Server	A virtual server must be created per port based on the Skype for Business edge pool external interface table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

Creating a Traffic IP Group for the Skype for Business Edge Pool External Interface (Access Edge) Pool

Create a traffic IP group for the edge pool external interface (Access Edge) pool (also known as the virtual IP) for each pool managed by the Virtual Traffic Manager. Per the earlier table, start by creating the 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., sfb-EII-pool.company.com for the edge pool external interface [Access Edge]pool)
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers

3. Click **Create IP Traffic Group**.

Skype for Business Edge Pool External Interface (Access Edge) Pools

Next create the edge pool external interface (Access Edge) pools. These pools manage many Skype for Business services and, as a result, use many ports. The Skype for Business Edge External Interface (Access Edge) Table on page 28 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. The port is listed in the first column of the previous configuration tables. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).
3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table, and click **Update**.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external Access Edge pools, edge external Web Conferencing services pools, and edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   If you need to create additional persistence classes based on the note above, perform the following steps:

   1. Select **Catalogs** > **Persistence**.
   2. Scroll down and create a new session persistence class.
   3. Set the type according to the entry in the configuration table.

Attaching the Session Persistence Class to a Pool

1. Navigate to **Services** > **Pools**, and select the pool that the monitor will be attached to.
2. Scroll down, click **Session Persistence.**
3. Choose the appropriate session persistence class.

   The following table contains a list of the Skype for Business services on the edge pool external interface (Access Edge) pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (six pools in total).

Skype for Business Edge External Interface (Access Edge) Table

The following table contains a list of the Skype for Business services on the external interface of the edge pool along with the Virtual Traffic Manager settings. A new port, XMPP, is used to allow communication with XMPP federated partners.

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
443	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	SIP/TLS
5061	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	SIP/TLS
5269	SSL (Other)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	(Optional) XMPP

Creating the Skype for Business Edge External Interface (Access Edge) Virtual Servers

Each pool must be associated with a virtual server, one to match each pool created in the previous section. 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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Default Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

Skype for Business External Interface (Web Conferencing Services) Service Configuration

The Skype for Business Web Conferencing service running on the edge pool has its own set of IP addresses, allowing for port overlap. The Skype for Business External Interface (Web Conferencing Services) Table on page 30 is used in this section.

Component	Procedure	Description
External Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created for web conferencing on the external interface of the Skype for Business edge pool.
External Virtual Traffic Manager (repeat for each row in the Skype for Business External Interface (Web Conferencing Services) Table on page 30)	Creating a Pool	A pool must be created per port. The IP address for the Web Conferencing services on each individual Skype for Business edge server must be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Create an IP-based persistence class for the pool.

Component	Procedure	Description
	Configuring the TCP Connect Health Monitor	Configure the TCP connect health monitor for the pool.
	Creating a Virtual Server	A virtual server must be created per port in the Skype for Business edge pool external interface (Web Conferencing) table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

Creating a Traffic IP Group for the Skype for Business External Interface (Web Conferencing Services) Service Pool

Create a traffic IP group for the external interface (Web Conferencing services) service pool (also known as a virtual IP) for each pool managed by the Virtual Traffic Manager. Per the earlier table, start by creating the 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., sfb-EII-pool.company.com for the external interface [Web Conferencing services] service pool
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business External Interface (Web Conferencing Services) Service Pools

Next create the external interface (Web Conferencing services) service pools. These pools manage many Skype for Business services and, as a result, use many ports. The Skype for Business External Interface (Web Conferencing Services) Table on page 30 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. The port is listed in the first column of the previous configuration tables. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).

3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table, and click **Update**.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external Access Edge pools, edge external Web Conferencing services pools, and the edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   If you need to create additional persistence classes based on the note above, perform the following steps:

   1. Select **Catalogs** > **Persistence**.
   2. Scroll down and create a new session persistence class.
   3. Set the type according to the entry in the configuration table.

Attaching the Session Persistence Class to a Pool

1. Navigate to **Services** > **Pools**, and select the pool that the monitor will be attached to.
2. Scroll down, click **Session Persistence.**
3. Choose the appropriate session persistence class.

   The following table contains a list of the Skype for Business services on the external interface (Web Conferencing services) service pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (six pools in total).

Skype for Business External Interface (Web Conferencing Services) Table

If using web conferencing services on the Skype for Business edge pool external interface, the following additional port must be configured. The Skype for Business Web Conferencing service running on the edge pool has its own set of IP addresses, allowing for port overlap.

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
443	SSL (HTTPS)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Remote user access

Creating the Skype for Business Edge External Interface (Web Conferencing Services) Virtual Servers

Each pool must be associated with a virtual server, one to match each pool created in the previous section. 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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Default Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

Skype for Business External Interface (A/V Services) Service Configuration

IP transparency is disabled by default. Only ports 443 and 5061 of the Skype for Business A/V service must be modified.

1. Navigate to **Services** > **Pools**, and select the pool corresponding to port 443 or 5061.
2. When configuring ports 443 and 5061, scroll down, click **Connection Management**, and click **Edit**.
3. Under **IP Transparency**, set transport to **Yes**, and click **Update**.

   If using A/V services on the Skype for Business edge pool external interface, the following additional ports must be configured. The Skype for Business A/V service running on the edge pool has its own set of IP addresses, allowing for port overlap. The Skype for Business External Interface (A/V Services) Table on page 33 is used in this section.

Component	Procedure	Description
External Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created for A/V services on the external interface of the Skype for Business edge pool.
External Virtual Traffic Manager (repeat for each row in the Skype for Business External Interface (A/V Services) Table on page 33)	Creating a Pool	A pool must be created per port. The IP address for A/V services on each individual Skype for Business edge server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Configure IP-based session persistence for the pool.
	(Only required for port 443) Configuring the TCP Connect Health Monitor	Configure the TCP connect health monitor for the pool.
	Enabling IP Transparency on the Pool	Skype for Business A/V services require IP transparency.
	Creating a Virtual Server	A virtual server must be created per port based on the Skype for Business edge pool external interface (A/V Services) table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

Creating a Traffic IP Group for the Skype for Business External Interface (A/V Services) Service Pool

Create a traffic IP group for the external interface (A/V services) service pool (also known as a virtual IP) for each pool managed by the Virtual Traffic Manager. Per the earlier table, start by creating the 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., sfb-EII-pool.company.com for the external interface (A/V services) service pool
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business External Interface (A/V Services) Service Pools

Next create the external interface (A/V services) service pools. These pools manage many Skype for Business services and, as a result, use many ports. The Skype for Business External Interface (A/V Services) Table on page 33 is used in this section. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).
3. Repeat for each pool needed, for each port in the table that follows.

Skype for Business External Interface (A/V Services) Load Balancing

Once a pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

1. Scroll down, click **Load Balancing**, and click **Edit**.
2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
3. Scroll down and click **Session Persistence**.

4. Choose the appropriate session persistence class based on the table, and click **Update**.

   NOTE
   Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external Access Edge pools, edge external Web Conferencing services pools, and edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

   If you need to create additional persistence classes based on the note above, perform the following steps:

   1. Select **Catalogs** > **Persistence**.
   2. Scroll down and create a new session persistence class.
   3. Set the type according to the entry in the configuration table.

Attaching the Session Persistence Class to a Pool

1. Navigate to **Services** > **Pools**, and select the pool that the monitor will be attached to.
2. Scroll down, click **Session Persistence**.
3. Choose the appropriate session persistence class.

   The following table contains a list of the Skype for Business services on the external interface (A/V services) service pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (six pools in total).

Skype for Business External Interface (A/V Services) Table

If using A/V services on the Skype for Business edge pool external interface, the following additional ports must be configured. The Skype for Business A/V service running on the edge pool has its own set of IP addresses, allowing for port overlap.

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
443	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	Yes	External Access to A/V (TCP)
3478	UDP	Least Connections	IP-Based Persistence	None	Yes	External Access to A/V (UDP)

Creating Skype for Business External Interface (A/V Services) Virtual Servers

Each pool must be associated with a virtual server, one to match each pool created in the previous section. 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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Default Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.

4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

Skype for Business Director Pool Service Configuration

The Skype for Business director pool can improve the performance of the front-end pool by offloading user authentication. The director role is now optional in Microsoft Skype for Business Server 2015 to reduce server count and other hardware requirements; however, it is still possible to load-balance the director pool if an administrator wants to take advantage of its role. The Skype for Business Director Pool Table of Services on page 35 is used in this section.

Each of the following elements must be created for the edge internal interface service configuration.

Component	Procedure	Description
Internal Virtual Traffic Manager (once)	Creating a Traffic IP Group	A single traffic IP group must be created to front the Skype for Business director pool.
Internal Virtual Traffic Manager (repeat for each row in the Skype for Business Director Pool Table of Services on page 35)	Creating a Pool	A pool must be created per port. The IP address of each individual Skype for Business director server should be added to the pool.
	Changing the Load-Balancing Algorithm on the Pool to Least Connections	The default Virtual Traffic Manager load-balancing algorithm is Round Robin. It should be changed to Least Connections.
	Configuring IP-Based Session Persistence on the Pool	Configure IP-based session persistence for the pool.
	Configuring the TCP Connect Health Monitor	Configure the TCP connect health monitor for the pool.
	Creating a Virtual Server	A virtual server must be created per port based on the Skype for Business director pool table.
	Changing the TCP Timeout on the Virtual Server to 1200 Seconds (20 Minutes)	The default TCP timeout is 300 seconds and should be changed to 1200 seconds.

Creating a Traffic IP Group for the Director Pool

Create a traffic IP group for the director pool (also known as a virtual IP) for each pool managed by the Virtual Traffic Manager. Per the earlier table, start by creating the 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., sfb-fe-pool.company.com for the director pool)
   - **IP Addresses**—A list of IP addresses separated by commas
   - **IP Mode**—How IP addresses are raised on the Virtual Traffic Managers
3. Click **Create IP Traffic Group**.

Skype for Business Director Pool

Next create the director pool. A pool must be created for each service/port managed by the Virtual 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 (or IP address): port for each of the actual back-end nodes. Multiple nodes can be entered with a space between them.
   - **Monitor**—Set to **TCP Connect Monitor** (or for optional HTTP 8080, choose the custom HTTP monitor).
3. Repeat for each pool needed, for each port in the table that follows.

   Once the pool is created, change the load-balancing algorithm for that pool. The default Virtual Traffic Manager load-balancing algorithm is Round Robin. All Skype for Business services require the load-balancing algorithm to be Least Connections.

   1. Scroll down, click **Load Balancing**, and click **Edit**.
   2. Set the loading-balancing algorithm to **Least Connections**, and click **Update**.
   3. Scroll down and click **Session Persistence**.
   4. Choose the appropriate session persistence class based on the table, and click **Update**.

      NOTE
      Multiple persistence classes may be created for pools that have differing nodes routing to different IP addresses. For example, the edge external Access Edge pools, edge external Web Conferencing services pools, and edge external A/V services pools are all hosted on the same Virtual Traffic Manager and use IP-based persistence but route to different nodes. In this case, create three IP-based persistence classes, one for each pool, and use the corresponding persistence class for each pool. Attempting to assign only one IP-based persistence class is not allowed.

      NOTE
      The following table contains a list of the Skype for Business services on the director pool along with the necessary Virtual Traffic Manager settings. You must create a pool for each port, with all nodes added to it (16 pools in total).

Skype for Business Director Pool Table of Services

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
443	SSL (HTTPS)	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Communication with web farm
444	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Communication with Skype for Business front end
5061	Generic Client First	Least Connections	IP-Based Persistence	TCP Connect Monitor	No	Used for internal communications

Creating Skype for Business Director Pool Virtual Servers

Each pool must be associated with a virtual server. 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**—Listed in the second column of the previous configuration table.
   - **Port**—Listed in the first column of the previous configuration table. This port will match the port configured in the corresponding pool.
   - **Default Traffic Pool**—Select the pool created in the previous section that matches the port for this VIP.
3. Set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

   The default Virtual Traffic Manager TCP timeout is 300 seconds (5 minutes). All Skype for Business TCP services require a TCP timeout of 1200 seconds (20 minutes).

   1. Scroll down, select **Connection Management**, and click **Edit**.
   2. Under **Timeout Settings**, change the timeout to **1200**, and click **Update**.

Configuring SSL Decryption and Encryption

If configuring only Skype for Business Server 2015 deployments and subsequently using only IP-based persistence, there is no need to configure SSL decryption and encryption; however, if there are existing Lync Server 2010 servers in the Skype for Business Server 2015 deployment and transparent session affinity is used, it is necessary to configure SSL decryption and encryption. This configuration allows a cookie to be inserted to maintain session persistence. This section details the steps to perform SSL decryption and re-encryption.

Importing the Certificate

To perform SSL decryption, the certificate and the private key used by the Skype for Business server must be imported into the Virtual Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates**.
2. Click **Import Certificate** to import the appropriate certificate. Refer to Common Troubleshooting Tips on page 47 for more details on importing certificates to the Virtual Traffic Manager.

Enabling SSL Decryption on the Virtual Server

After importing the certificate, enable SSL decryption on the virtual server created.

1. Navigate to **Services** > **Virtual Servers**, and select the virtual server that will perform SSL decryption.
2. Scroll down, and click **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in Step 2 of Importing the Certificate on page 36.

Enabling SSL Encryption on the Pool

This section details the steps to perform SSL encryption to re-encrypt the SSL session to the back-end node.

1. Navigate to **Services** > **Pools**, and select the pool on which SSL encryption will be enabled.
2. Scroll down, and click **SSL Settings**.

3. Set **ssl_encrypt** to **Yes**.

DNS Load Balancing

Microsoft optimized Skype for Business 2015 to be used in conjunction with DNS load balancing and recommends this technology when load-balancing functionality is needed for an edge pool. DNS load balancing is defined as a method of load balancing where a list of IP addresses is returned in response to a DNS query. The client picks one of the provided IP addresses by random; however, there are three scenarios where DNS load balancing cannot provide a working solution. Microsoft therefore recommends the use of an application delivery controller, such as Brocade's Virtual Traffic Manager, or a hardware load balancer to provide load balancing in the following scenarios:

- Federation with organizations using Office Communications Server 2007 R2 or Office Communications Server 2007
- Exchange UM for remote users using Exchange UM prior to Exchange 2010 with SP1
- Connectivity to public IM users

For further information about DNS load balancing and the specific scenarios for application delivery controller/hardware load balancer, refer to the following links:

- DNS Load Balancing
- Hardware Load Balancer Requirements

Configuring Office Web Apps Server for Virtual Traffic Manager

This chapter provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for Microsoft Office Web Apps 2013. Office Web Apps 2013 is a web-based version of the Microsoft Office suite that can integrate with Exchange, Skype for Business, and SharePoint. In a typical Skype for Business deployment, Office Web Apps servers are also deployed and integrated with Skype for Business 2015. Use these instructions to configure the Virtual Traffic Manager to load-balance Office Web Apps 2013.

Microsoft Office Web Apps 2013 can be configured to allow SSL offloading. For more information, refer to the TechNet article at https://technet.microsoft.com/en-us/library/jj219435.aspx.

Creating a Traffic IP Group for Office Web Apps 2013

Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen. 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 SharePoint farm site (e.g., officeweb.mycompany.com)
   - **IP Addresses**—An IP address that is mapped to the FQDN of the SharePoint farm site
3. Click **Create Traffic Group**.

Creating a Pool That Contains Office Web Apps Servers

A pool must be created for the Office Web Apps service managed by the Virtual 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 (e.g., Office Web Apps)
   - **Nodes**—**hostname: 80** or **ipaddress: 80** (Note: Use port 443 if SSL offloading is not configured on Office Web Apps servers.)
   - **Monitor**—**Full HTTP** (Note: Use **Full HTTPS** if SSL offloading is not configured on Office Web Apps servers.)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Least Connections**.
5. Click **Update** to apply the changes.

Configuring Session Persistence for the Office Web Apps Pool

The section describes how to configure transparent-session-affinity-based session persistence on the pool created in the previous procedure.

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **Transparent session affinity** in **Basic Settings**.
5. Click **Update** to apply changes.
6. Navigate to **Services** > **Pools**, and select the appropriate pool that was created earlier.
7. Navigate to **Session Persistence**, and click **Edit**.
8. Select the session persistence class created, and click **Update** to apply the changes.

Creating a Virtual Server That Listens to the Office Web Apps Traffic IP Group

Create a virtual server that will handle all the view client 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 (e.g., sp.mycompany.com)
   - **Protocol**—**HTTP** (Note: Use **SSL HTTPS** if SSL offloading is not configured on Office Web Apps servers.)
   - **Port**—**443**
   - **Default Traffic Pool**—The pool created for this service earlier
3. Click **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 **Update** to apply changes.

Configuring SSL Decryption for SSL Offloading

Perform the procedures in this section only if SSL offloading is configured for Office Web Apps servers.

Importing the Certificate

To perform SSL decryption, the certificate and the private key used for the Lync server created previously must be imported into the Virtual Traffic Manager.

1. Navigate to **Catalogs** > **SSL** > **SSL Certificates catalog**.

2. Click **Import Certificate** to import the appropriate certificate.

Enabling SSL Decryption on the Virtual Server

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 SharePoint farm website that will perform SSL decryption.
2. Scroll down, and click **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in Step 2 of Importing the Certificate on page 40.
5. Scroll down to the bottom of the page, and click **Update**.

Using Virtual Traffic Manager to Enhance a Microsoft Skype for Business 2015 Deployment

Brocade's Virtual Traffic Manager has additional capabilities beyond a legacy load balancer to enhance the performance and manageability of your Microsoft Skype for Business 2015 environment. Here are some common capabilities and best practices for deploying the Virtual Traffic Manager to enhance your Microsoft Skype for Business 2015 deployment.

Service-Level Monitoring

This feature monitors the responses of your SharePoint servers and can send alerts should these responses fall below an expected threshold of performance. In addition to sending alerts, a TrafficScript rule can be written and configured to remove the service or server from the pool until the performance issue has been remediated, to reprioritize traffic, and even to reallocate bandwidth. Essentially, by using a TrafficScript rule for service-level monitoring, services can be controlled and managed.

Global Load Balancing

Global load balancing enables clients to be distributed across multiple locations, either for Disaster Recovery (DR) or based on their geographic proximity to a data center. As a common issue when failing over to a DR location, services become unavailable until the DNS Time-to-Live (TTL) expires, so that clients can resolve the IP address of the DR location. Configuring the Virtual Traffic Manager for global load balancing using active/passive mode improves and utilizes failover Recovery Time Objective (RTO) because vTM is no longer constrained by the DNS TTL.

In the case of Skype for Business 2015, aside from DNS, additional PowerShell commands should be run on a Skype for Business server to fail over to another active pool. This process can be automated by integrating Virtual Traffic Manager with PowerShell. One way to do so is to create custom health monitors for a traffic IP group and a virtual server, which PowerShell monitors.

```
#// Script for Monitoring TCP Port 80
$debug = 0; // Change value to 1 if debug needed
$sock = tcp.connect( "192.168.1.26", 80, 200);
if( ! $sock )
{
   http.sendResponse("200 OK", "text/html", "NOK", "");
   if ($debug > 0) { log.info("Send NOK");}
}
else
{
   tcp.close( $sock );
   http.sendResponse("200 OK", "text/html", "OK", "");
      if ($debug > 0) { log.info("Send OK");}
}
```

Using PowerShell scripting and job monitoring, the process of moving clients to another active pool can be automated based on the response of the Virtual Traffic Manager: "OK" or "NOK" as shown in the previous example. The following is a sample PowerShell script that retrieves the response of the health monitor by accessing the FQDN of the traffic IP group.

```
$health = (new-object net.webclient).DownloadString("http://monitor.mycompany.com")
```

Skype for Business Web Client Supported Web Browsers

TrafficScript in the Virtual Traffic Manager can be used to detect whether the client's browser supports the Skype for Business web client and redirects unsupported clients to another website showing a notification that the current browser will not be able to provide the full feature or functionality of the Skype for Business web client. A TrafficScript is then assigned to a virtual server to leverage the script for monitoring. See the following sample TrafficScript code:

```
#// TS Rule for redirecting HTTP requests based on client
$browser = http.getHeader("user-agent");
#// Set the Debug Level (possible values: 0,1,2,3)
#// 0 = Logging Off
#// 1 = Informational logging
#// 2 = Full Debug
$debug = 2;

if(string.contains ($browser, "MSIE 6.0"))
{
   http.redirect("http://www.brocade.com");

    #or uncomment the line below and delete the line above
#http.sendResponse( "400 Bad Request", "text/plain","Bad Request", "");
   if ($debug > 0) { log.info("Client Redirected");}
}
```

Configuring Clustering for Virtual Traffic Manager

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

Perform the following steps to join a Virtual Traffic Manager to an existing cluster.

1. Navigate to **System** > **Traffic Managers**.
2. Scroll down to **Add or Remove Traffic Managers**, and click **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, provide a username and password for the cluster, and click **Next** to continue.
6. Select **Yes**, allow it to host traffic IPs immediately, and click **Next**.
7. In the **Summary** page, click **Finish** to join the vTM to the cluster.

Virtual Web Application Firewall

Brocade Virtual Web Application Firewall (Brocade vWAF) is a scalable security platform for off-the-shelf solutions and custom applications. Brocade vWAF lets you apply business rules to online traffic, screening for attacks such as SQL injection and cross-site scripting (XSS), while securing outgoing traffic to help comply with PCI-DSS and HIPAA. Brocade vWAF can be run as an add-on to the vTM to enable both load balancing and application firewall services on a single instance.

Apart from custom rule configurations that are possible on the vWAF, there is a ruleset called baseline protection that protects applications from the most common application-layer attacks that exist today, such as the following:

- Path Traversal
- Shell Command Injection
- SQL Injection
- Code Injection
- Cross-Site Scripting (XSS)
- Common Attacks
- LDAP Injection
- Scanner
- XPATH Injection

The following procedure documents the configuration of the Brocade Virtual Web Application Firewall for baseline protection of the Microsoft Skype for Business application for the HTTP services.

1. On the vTM, navigate to **System > Application Firewall**, and click the **afm_enabled** radio button, followed by **Update** (ensure that the **Confirm** checkbox is checked).
2. Click the **Application Firewall** tab on the vTM.
3. Click **Administration**, and then select **Baseline Management**.
4. From this screen, either download the latest Virtual Web Application Firewall baseline signatures from Brocade Communities and click **Upload** or click the **Download from Server** option if your vTM+vWAF has Internet connectivity.
5. In the **Application Firewall** UI, click **Application Control** and select **Application Creation Wizard**.
6. Enter a name for the application, and click **Continue**.
7. Choose the detection mode that will enable the firewall rules to be applied to production traffic. Choose the protection mode for not affecting production traffic and whether you want to test the rules and check the logs for their accuracy. Click **Continue**.
8. In the **customer key** screen, leave the default, and click **Continue**.
9. In the **hostname** screen, enter the exact FQDN/IP address (typically this is the TIP group address) by which users/clients will access the application. You can enter multiple values for one application simply by clicking **Add hostname** after adding one. Click **Continue**.
10. In the next screen, leave the default logging level to reduced logging unless there is a need to monitor the complete logs. Click **Continue**.
11. In the next screen, choose the option to enable full request logging and selecting the number of days for data retention. If indefinite, leave it to the default **0**. Click **Continue**.
12. In the next screen, choose to run the **Baseline Protection** wizard. Click **Continue**, and then click **Finish**.
13. In the **Baseline Protection** wizard, click **Next** on the **Overview** screen.
14. Choose the baseline version to use. Click **Next**.

15. Leave the rest of the screens to their defaults, and, finally, click **Finish**.
16. Click the **Virtual Traffic Manager** tab to go back to the vTM UI.
17. Select the virtual server on which the vWAF service is to be enabled, and select **enabled** for the **Application Firewall** option, and click **Update**.

    You can reach out to the Brocade support team for help on more advanced and customized configuration of the Virtual Web Application Firewall.

Common Troubleshooting Tips

Common Deployment Issues

This section describes some common issues that can arise when deploying Microsoft Skype for Business 2015 along with the Brocade Virtual Traffic Manager and ways to resolve these issues.

Checking DNS Entries

The most likely reason that Skype for Business is not able to sign in is missing DNS records. A proper Skype for Business deployment requires a number of DNS entries.

- Make sure that the DNS requirements for Skype for Business are completed. The DNS requirements can be found here: https://technet.microsoft.com/en-us/library/dn951397.aspx.
- In a default Skype for Business Server 2015 deployment, the DNS entries are configured to point directly to their corresponding pools such as the front-end pool and the edge pool; however, for the Virtual Traffic Manager deployment, make sure that these DNS entries point to the virtual IP (the traffic IP group) of the virtual server load-balancing the specific pool. This will ensure that the traffic goes to the Virtual Traffic Manager for load balancing.

Certificates

Another common reason that the Skype for Business client cannot sign in is an invalid certificate on the vTM. If using a firewall/reverse proxy, the vTM must be able to decrypt SSL traffic, requiring a certificate and a private key to do so. If you are using an internal Certificate Authority (CA), Step 3 of the Skype for Business Server Deployment Wizard can automatically generate a certificate request to the internal CA, but the default settings will mark the private key as not exportable. To properly generate a certificate with an exportable private key:

1. After selecting **Step 3: Request, Install, or Assign Certificates > Run > Request**, select **Prepare the request now, but send it later**.
2. After stepping through a few screens, there will be an option to **Mark the certificate private key as exportable**. Make sure that the checkbox is checked.
3. On the **Configure Additional Subject Alternate Names** page, fill in all FQDNs created for all pools. This will allow the same certificate to be used for all Skype for Business servers.
4. The result will be a certificate request in the form of a .csr file. Use that to request a certificate through the internal CA.
5. Import the certificate into any Skype for Business server.
6. From that same Skype for Business server, export the certificate with the private key.
7. Import the certificate to all Skype for Business servers and the vTM.

Importing Certificates into Virtual Traffic Manager

Virtual Traffic Manager requires a PEM certificate file format to be uploaded into the system. There are available tools to convert CER (without a key) and PFX (with a key) formats to PEM format, such as OpenSSL. To upload a certificate used by a Skype for Business server, export the certificate once with a private key and once without a private key. Use the following command 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
```

Clients Are Connecting Directly to the Skype for Business Servers

The Skype for Business client can sign in, but it goes directly to a Skype for Business front-end server without going through the vTM. This is expected behavior. The Skype for Business clients will initially go through the vTM for authentication but will then be redirected to their home server, which is determined by the Skype for Business client's SIP URI. This behavior is discussed in the "Client Registration" section of the following TechNet article:

https://blogs.technet.microsoft.com/nexthop/2011/05/25/dns-load-balancing-in-lync-server-2010/

The article is for Lync Server 2010 but is applicable to Skype for Business Server 2015.

Virtual Traffic Manager Shows Some Pools as Having an Error

If the Virtual Traffic Manager indicates that a pool has an error even though the respective server is still running, refer to the following tips to help troubleshoot this problem:

- Make sure that the firewall of the respective Skype for Business server is not blocking the specified ports used by the service involved. Microsoft Skype for Business Server 2015 automatically configures these firewall settings; however, it is important to make sure that the necessary ports are opened. Refer to the following TechNet article for the complete list of ports needed by Skype for Business Server 2015: https://technet.microsoft.com/en-us/library/gg398833.aspx.
- Make sure that the service is installed in Skype for Business Server 2015. There are some cases where some services are not installed properly. In order to check whether the service is running, go to the respective Skype for Business server and check Services.msc.

  You can also use SSH to connect to one of the Virtual Traffic Mangers and use the **telnet** command to see if a given service is reachable by the Virtual Traffic Manager. For example, you can run the **telnet <Skype for Business server IP> 5073** command on a Virtual Traffic Manager directly to verify if one of the ports on the Skype for Business front-end pool is running properly.

Other Troubleshooting Tips

This section contains some miscellaneous troubleshooting tips that are helpful when deploying Microsoft Skype for Business 2015 along with the Virtual Traffic Manager.

Checking Connections to the Virtual Traffic Manager

Follow the tips below to check whether the Virtual Traffic Manager was configured correctly and is accepting traffic:

- On the Virtual Traffic Manager, navigate to **Activity > Connections** and see whether connections are being made to the virtual servers. If not, either the Skype for Business client cannot reach the Virtual Traffic Manager or Skype for Business is connecting directly to the respective pools because of DNS entries. Activity connections monitoring is not enabled by default. To enable the tracing for a virtual server:
  1. Navigate to **Services > Virtual Server**, and select the virtual server where tracing will be enabled.
  2. Set **Request Tracing** to **Yes** and click **Update**.
  3. Log configurations can be done through **System > Global Settings Logging**.
- Install Wireshark on the Skype for Business client machine and see how far the Skype for Business client gets. If the client is sending out DNS requests for _sipinternaltls._tcp.<domain> or similar FQDNs and not getting responses, see the "Check DNS Entries" section.
- Enable client-side logging on the Skype for Business client. This is helpful for observing the connections that the Skype for Business client attempted and the errors that it encountered. To enable client-side logging, perform these steps:
  1. In the upper right corner of the Lync server main window, click **Options (gear icon**).
  2. In the **Skype for Business - Options** dialog box, click **General**.
  3. Under **Logging**, check the **Turn on logging in Skype for Business** and **Turn on Windows Event logging for Skype for Business** checkboxes.
  4. Click **OK**.
  5. Restart Skype for Business, and then try to reproduce the issue.

Session Persistence Error When Configuring a Persistence Class

When configuring a session persistence class, the following error may be generated:

```
ERROR: This persistence class is being used by other pools with different node addresses, which can
cause problems with session affinity. Please create a new persistence class and assign that
instead.
```

This message occurs because the pool that is trying to be used has completely different IP addresses than the one that this persistence class is already used for.

For example, if the node that is being balanced to has a 10.255.1.X/24 address and the other nodes in the same persistence class have a 10.255.2.X/24 address, then a persistence class must be created for the new node on a different subnet. In short, a persistence class must be created for each subnet.

If this is the case, create a new persistence class of type IP-Based, with a different name, and use that for the specific nodes on the alternate subnet:

1. Select **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **IP-Based Persistence** under **Basic Settings**.
5. Click **Update** to apply changes.
6. Select **Services** > **Pools**, and choose the appropriate pool created earlier.

7. Select **Session Persistence**, and click **Edit**.
8. Select the session persistence class just created, and click **Update** to apply changes.

Address in Use Error When Adding a Pool

When pools are turned on after creation, an error like the following may be generated:

```
port: Failed to bind to XXX.XXX.XXX.XXX:port# (Address already in use)
```

This error is generated because the VIP is trying to bind on a port and address that is already in use on the interface of the Virtual Traffic Manager. In this case, perform the following steps:

1. Select **Home**, and choose the virtual server in error.
2. Expand **Basic Settings**, and select **Traffic IP Groups**.
3. Check the **Select** checkbox that has the specific traffic IP group to be used with this IP group.
4. Click **Update**.

   NOTE
   These steps may need to be performed on both virtual servers that are failing to bind on the problematic port. These steps can also be performed on all virtual servers to specifically bind them to traffic IP groups.

Diagnose Tab in Virtual Traffic Manager

The **Diagnose** tab in the Virtual Traffic Manager is a useful tool that shows the summary of all current problems in the configuration. Additionally, it shows a description for each specific error, making it easier to identify the problem.

Conclusion

This document briefly discusses how to configure Virtual Traffic Manager to optimize the Microsoft Skype for Business 2015 deployment. Virtual Traffic Manager can make intelligent load-balancing decisions and improve the performance, security, reliability, and integrity of the traffic in this environment. Refer to the product documentation on the Brocade Community Forums (http://community.brocade.com) for examples of how Brocade Virtual Traffic Manager can be deployed to meet a range of service-hosting problems.

Appendix: Microsoft TechNet Resources

Hardware Load Balancer Requirements for Skype for Business 2015

https://technet.microsoft.com/en-us/library/gg615011.aspx

New Server Features in Skype for Business 2015

https://technet.microsoft.com/en-us/library/dn933785.aspx

Port Requirements in Skype for Business 2015

https://technet.microsoft.com/en-us/library/gg398833.aspx

Technical Requirements for Mobility

http://technet.microsoft.com/en-us/library/hh690030.aspx

Environmental Requirements for Skype for Business 2015

https://technet.microsoft.com/en-us/library/dn933910.aspx

Domain Name System (DNS) Requirements

https://technet.microsoft.com/en-us/library/dn951397.aspx

DNS Load Balancing in Lync Server 2010

http://blogs.technet.com/b/nexthop/archive/2011/05/25/dns-load-balancing-in-lync-server-2010.aspx

Changes in Lync Server 2013 That Affect Edge Server Planning

http://technet.microsoft.com/en-us/library/jj204965.aspx

Plan for High Availability and Disaster Recovery in Skype for Business Server 2015

https://technet.microsoft.com/en-us/library/dn933905.aspx

OpenSSL

http://gnuwin32.sourceforge.net/packages/openssl.htm