BROCADE

DEPLOYMENT GUIDE

Brocade Virtual Traffic Manager and Microsoft Lync 2010 Deployment Guide

53-1003964-02
13 March 2017

Contents

Preface

About This Guide

The *Brocade Virtual Traffic Manager and Microsoft Lync 2010 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft Lync 2010.This deployment guide includes information relevant to the following products: Brocade Virtual Traffic Manager and Microsoft Lync 2010. For more details on the Brocade vADC product family, see http://www.brocade.com/vADC.

Audience

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

- Microsoft Lync 2010 port requirements for both front-end and edge pools
- Installing and configuring a virtual appliance in a virtual VMware, 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
September 2015	53-1003964-01	Initial release.
March 2017	53-1003964-02	Added vWAF content.

Solution Overview

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 Brocade 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.

Microsoft Lync 2010

Microsoft Lync 2010 is a unified communications platform providing instant messaging, voice, video, and application sharing for both internal and external users. Each server in a Lync deployment provides a portion of the overall Lync functionality; and each server can be scaled to a pool of servers load-balanced by Brocade vTM. This deployment guide provides the steps necessary for vTM to load-balance the following Lync pools:

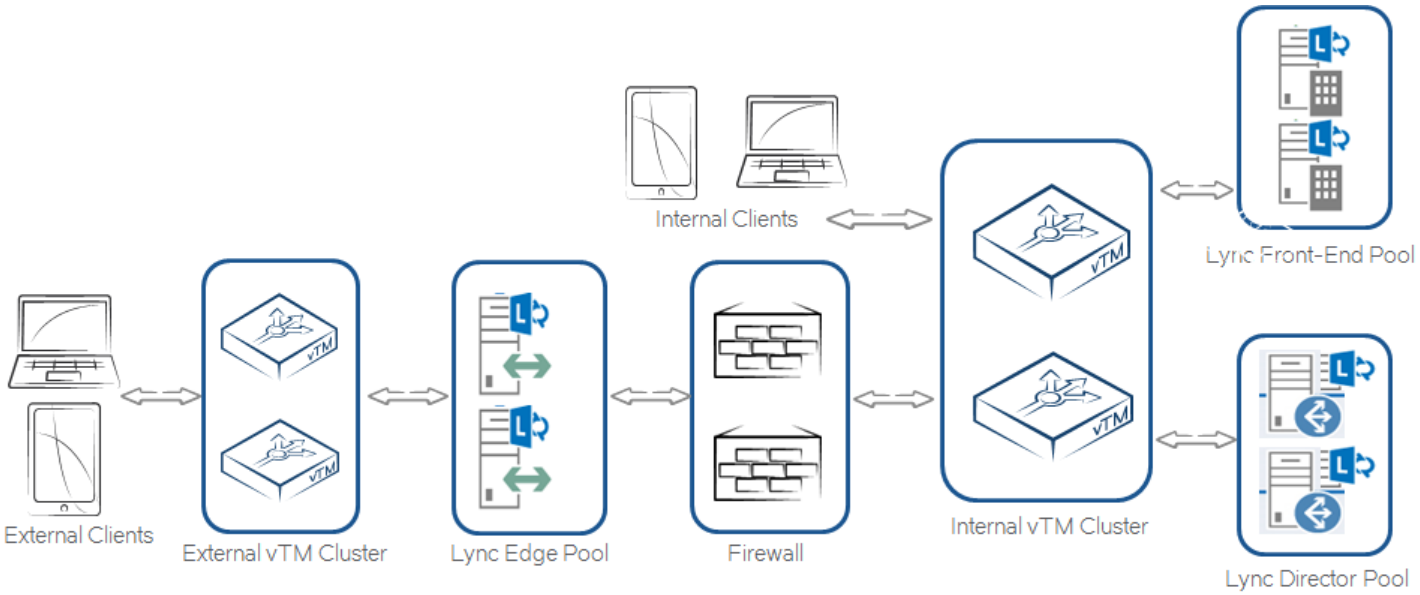
- **Front-End Pool**—The main Lync pool that handles authentication, instant messaging, and various other services.
- **Director Pool**—Offloads authentication of users from the front-end pool.
- **Edge Pool**—Allows external users to access Lync. They can be remote users or users from another organization, controlled by policy.

For each pool, a list of ports is provided along with the load-balancing algorithm, health monitor, persistence profile, and IP transparency setting to use with each port.

Microsoft Lync 2010 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 Lync edge pool and the other managing the internal interface of the Lync edge pool, the Lync front-end pool, optional Lync director pool, and firewall (reverse proxy).

An alternative deployment would be to have a single vTM cluster managing all traffic; this deployment is documented in Appendix B.

Deploying Brocade Virtual Traffic Manager and Microsoft Lync 2010

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft Lync 2010 Server

Understanding the Deployment Process

This section steps through the procedures to configure vTM to properly manage Lync traffic. Each Lync port on each server requires a new service to be entered into the Virtual Traffic Manager. The following services are needed:

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

Component	Procedure	Description
External Traffic Manager (for each service)	Creating a Traffic IP Group	Create a traffic IP group for each pool. For details, see Creating Traffic IP Groups on page 11.
	Creating a Pool	A pool must be created per service. The IP address for the external interface on each individual server should be added to the pool. For details, see Creating Pools on page 11.
	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. For details, see Changing the Load-Balancing Algorithm on page 11.
	Configuring Session Persistence on the Pool	For details, see Configuring Session Persistence on page 12.

Component	Procedure	Description
	Configuring IP Transparency	For details, see Configuring IP Transparency on page 12.
	Creating a Health Monitor	For details, see Creating Health Monitors on page 12.
	Creating a Virtual Server	A virtual server must be created per pool. For details, see Creating Virtual Servers on page 13.
	Changing the TCP Timeout on the Virtual Server to1200 seconds (20 minutes).	The default TCP timeout is 300 seconds and should be changed to 1200 seconds. For details, see Changing the TCP Timeout on page 14.
	Configuring SSL Decryption and Encryption	For details, see Configuring SSL Decryption and Encryption on page 14.

Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) for each pool managed by the vTM. For Lync, this includes:

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

Up to six unique traffic IP groups must be created. To create a new traffic IP group.

1. Navigate to **Services** > **Traffic IP Groups**, and scroll down to **Create a new Traffic IP Group**.
2. Fill in the fields as follows:
   - **Name**—A descriptive name for the traffic IP group, e.g., lync-fe-pool.company.com for the front-end pool.
   - **IP Addresses**—A list of IP addresses separated by spaces.

Creating Pools

For each service managed by the Virtual Traffic Manager, create a pool using the following steps.

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:** *port* for each of the actual back-end nodes. The port is listed in the first column of the configuration tables in Appendix A.
   - **Monitor**—Leave as **Ping** for now. This will be changed in the Creating Health Monitors on page 12.

Changing the Load-Balancing Algorithm

The default vTM load-balancing algorithm is Round Robin. All Lync services require the load-balancing algorithm to be Least Connections.

1. Navigate to **Services** > **Pools**, and select one of the pools created earlier.

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

Configuring Session Persistence

All Lync services require some form of session persistence. This section details the steps to configure session persistence.

Creating a New Session Persistence Class

A session persistence class must be created only once per type of persistence. For Lync only, **IP-based persistence** and **Transparent session affinity** are used, so only two persistence classes must be created.

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

Attaching the Session Persistence Class to a Pool

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

Configuring IP Transparency

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

1. Navigate to **Services** > **Pools**, and select the pool corresponding to either port 443 or 5061.
2. Scroll down, and click **Connection Management**.
3. Under **IP Transparency**, set **transport** to **Yes**.

Creating Health Monitors

There are three different types of health monitors that must be created for Lync. The following sections detail the steps to create these health monitors.

Creating a TCP Connect Monitor

The basic TCP Connect monitor is used by most of the Lync services.

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 **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 being 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 change **use_ssl** to **Yes**.
6. Change the **path** to **/groupexpansion/service.svc**.
7. Change **body_regex** to **.***.

Creating an HTTP Monitor

The HTTP monitor is used for port 8080 on the Lync 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 **.***.

Attaching the Monitor to a Pool

After the monitors have been created, they must be attached to the appropriate pool.

1. Navigate to **Services** > **Pools**, and select the pool to which the monitor will be attached.
2. Scroll down, and click **Health Monitoring**.
3. Add the appropriate health monitor.

Creating Virtual Servers

Each pool must be associated with a virtual server. 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 configuration tables in Appendix A.
   - **Port**—Listed in the first column of the configuration tables in Appendix A. This port will match the port configured in the corresponding pool.
   - **Default Traffic Pool**—The pool created for this service earlier.

Changing the TCP Timeout

The default vTM TCP timeout is 300 seconds (5 minutes). All Lync TCP services require a TCP timeout of 1200 seconds (20 minutes).

1. Navigate to **Services** > **Virtual Servers**, and select the appropriate virtual server.
2. Scroll down, and select **Connection Management**.
3. Under **Timeout Settings**, change **timeout** to **1200**.

Configuring SSL Decryption and Encryption

A few of the Lync services that use SSL(see above) require vTM to first decrypt the SSL session and then re-encrypt it before sending it to the server; this so a cookie can 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 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 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 14.

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 for which SSL encryption will be enabled.
2. Scroll down, and click **SSL Settings**.
3. Set **ssl_encrypt** to **Yes**.

DNS Load Balancing

DNS load balancing is a method of load balancing where a list of IP addresses is returned in response to a DNS query. The client then picks a random IP address from the list and uses that. DNS load balancing has the benefit of being easy to deploy; typically a single SRV record with a list of IP addresses is added to the DNS server. DNS load balancing is supported in Lync for all non-HTTP-based traffic; for HTTP-based traffic, a load balancer such as vTM is still required. This is because DNS load balancing cannot provide session persistence; a server is randomly selected with each connection.

Lync can be deployed either using a mix of DNS load balancing and vTM load balancing or using just purely vTM load balancing. If the mixed deployment is used, only ports 80, 135, 443, 444, 5061, and 8080 must be configured on the vTM that manages the Lync front-end pool. Everything else remains the same.

Virtual Web Application Firewall

Brocade Virtual Web Application Firewall (Brocade vWAF) is a scalable security platform for off-the-shelf solutions and custom applications. It 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 Lync application for 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

This deployment guide covers most of the deployment scenarios, but sometimes sign-in or other problems may arise. This section steps through some of the common issues and ways to address them.

Check DNS Entries

The most likely reason that the Lync client is not able to sign in is missing DNS records. A proper Lync deployment requires a number of DNS entries. In addition to the FQDNs created for each pool during installation, a few additional DNS records are required.

- For internal Lync clients, a DNS SRV record of the format *_sipinternaltls._tcp.<domain>* pointing to the Lync front-end pool is required. This TechNet article (https://technet.microsoft.com/en-us/library/gg398680.aspx) discusses the steps to create this record.
- For external and mobile clients, a few additional DNS records are required. Refer to this TechNet article (https://technet.microsoft.com/en-us/library/hh690040).

Certificates

Another common reason that the Lync client is not able to 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 Lync 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 Lync 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 Lync server.
6. From that same Lync server, export the certificate with the private key. The certificate coming for the internal CA does not have a private key associated with it.
7. Import the certificate to all the Lync servers and vTM.

Clients Are Connecting Directly to the Lync Servers

The Lync client can sign in, but it goes directly to a Lync front-end server without going through the vTM. This is expected behavior. The Lync clients will initially go through the vTM for authentication but will then be redirected to their home server, which is determined by the Lync 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/

Other Troubleshooting Tips

This section contains a collection of general debugging tips.

- On vTM, navigate to **Activity > Connections** and see if connections are being made to vTM virtual servers. If not, the Lync client cannot reach the vTM.
- Install Wireshark on the Lync client machine and see how far the Lync client is getting. If it is sending out DNS requests for *_sipinternaltls._tcp.<domain>* or similar FQDNs and not getting responses, see Check DNS Entries.
- Follow this TechNet article (http://technet.microsoft.com/en-us/library/gg195661.aspx) to enable logging on the Lync client. Step through the logs to see if they provide any insight.

Conclusion

This document briefly discusses how to configure Brocade Virtual Traffic Manager to optimize Microsoft Lync 2010 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 A: Configuration Tables

This appendix contains configuration tables for the Lync front-end, Lync director, Lync edge, and reverse proxy pools. These configuration tables are referred to in the procedures within Deploying Brocade Virtual Traffic Manager and Microsoft Lync 2010 on page 10.

Lync Front-End Pool

The Lync front-end pool manages many Lync services, and thus it uses many ports. The following table contains a list of the Lync services on the front-end pool along with vTM settings.

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 Lync 2010 Attendant
5073	Generic Client First	Least Connections	IP-based Persistence	TCP Connect Monitor	No	(Optional) If using the Lync Server Conferencing Announcement service
5075	Generic Client First	Least Connections	IP-based Persistence	TCP Connect Monitor	No	Call Park application
5076	Generic Client First	Least Connections	IP-based Persistence	TCP Connect Monitor	No	Audio Test service

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
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	Transparent Session Affinity	HTTP Monitor	No	(Optional) Requires SSL encryption and decryption

Lync Director Pool

The Lync director pool can improve the performance of the front-end pool by offloading user authentication. The following table contains a list of the Lync services on the director pool along with vTM settings.

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 Lync front end
5061	Generic Client First	Least Connections	IP-based Persistence	TCP Connect Monitor	No	Used for internal communications

Reverse Proxy

If using a dual firewall DMZ deployment, an additional port must be added to the vTM. This port is for authentication, so it belongs first to the director pool if that is configured, otherwise to the front-end pool.

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
4443	HTTP	Least Connections	Transparent Session Affinity	HTTPS Monitor	No	Requires configuring SSL encryption and decryption

Lync Edge Pool

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

In this topology, we have two Virtual Traffic Manager clusters, one managing the external interface of the Lync edge pool and another managing the internal interface of the Lync edge pool, along with the Lync front-edge pool and optional Lync director pool.

Lync Edge Internal Interface

The following table contains a list of the Lync services on the internal interface of the edge pool along with vTM settings.

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

Port	Protocol	Load Balancing	Persistence	Health Monitor	IP Transparency	Notes
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

Lync Edge External Interface

The following table contains a list of the Lync services on the external interface of the edge pool along with vTM settings.

NOTE

The Lync Server 2010 edge external interface requires three public IP address for Virtual Traffic Manager 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 the "Choosing a Topology" section of Lync 2010 documentation on Microsoft TechNet. If the required number of public IP addresses cannot be secured, then DNS load balancing must be used instead since it supports NAT.

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
4443	HTTP	Least Connections	Transparent Session Affinity	HTTPS Monitor	No	For Lync Mobile. Requires configuring SSL encryption and decryption
8080	HTTP	Least Connections	Transparent Session Affinity	HTTPS Monitor	No	For Lync Mobile. Requires configuring SSL encryption and decryption

Web Conferencing Services

If using Web Conferencing Services on the Lync edge pool external interface, the following additional port must be configured. Lync Web Conferencing Services 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

A/V Services

If using A/V Services on the Lync edge pool external interface, the following additional ports must be configured. Lync A/V Services 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)

Appendix B: Alternative Topology

The alternative deployment shown in Figure 2 has a single vTM cluster that manages traffic to all servers. While easier to manage, this deployment is noticeably missing a DMZ. Although the internal clients are on the same network segment as the Lync pools, they will still run through the vTM for load balancing since the DNS entries for the various Lync pools will still point to the vTM. The configuration tables in Appendix A are still valid for this alternative configuration, with the main difference being that all services will be handled by a single vTM cluster instead of two.

FIGURE 2 Alternative Topology