DEPLOYMENT GUIDE

Thunder Series with Microsoft Lync Server 2013 for Reverse Proxy Deployments

Table of Contents

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

1 Introduction

A10 Networks® Thunder™ ADC product line of high-performance, next-generation application delivery controllers (ADCs) provides intelligent load balancing, security, acceleration and optimization for Microsoft Lync Server 2013.The Microsoft Lync integration with A10 Networks has been tested for both A10 Thunder hardware appliance models and vThunder™ hypervisor-based models based on the Unified Communication Open Interoperability Program (UCOIP) requirements

The purpose of this guide is to provide a step-by-step process on how to deploy the A10 Thunder ADC as a reverse proxy between external clients and a Microsoft Lync Server 2013 deployment. In addition, this guide offers instructions for configuring Thunder ADC security features, enabling Microsoft ForeFront Threat Management Gateway (TMG) customers to successfully transition from ForeFront TMG to A10 Thunder ADC.

In September 2012, Microsoft announced important changes to the ForeFront TMG roadmap, discontinuing any further releases of ForeFront TMG and announcing End of Support (EoS) dates for online service subscriptions and perpetual server licenses. As a result, ForeFront TMG customers need an alternative solution to secure their Microsoft Lync deployments. Thunder ADC, with its integrated reverse proxy and security features, provides the ideal migration option for ForeFront TMG customers. Thunder ADC, acting as a reverse proxy for Lync 2013, provides a single point of access and control for external clients. Thunder ADC provides comparable features such as reverse and forward proxy, high availability, Web Application Firewall (WAF), authentication, DNS firewall, and more.

The test environment is based on Microsoft Lync Server 2013 Enterprise edition. This guide can't be used for Microsoft Office Communication Server (OCS) 2007 R2 nor as a Lync Server 2010 deployment. Please refer to http://www.a10networks.com/resources/deployment_guides.php for additional Microsoft deployment guides.

The following topology (Figure 1) is designed to support Lync voice services, presence, instant messaging, desktop sharing, collaboration, and Enterprise Voice Features for both internal and external users with a high availability (HA) system architecture. In this guide, a Thunder ADC high availability pair is used to provision four (4) Layer 3 Virtualization (L3V) partitions to deploy four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy.

1.1 Lync Server 2013 Roles

The Lync Server 2013 solution requires multiple servers with distinct roles. The server roles are described below.

Front End Servers (Lync Servers)

The Front End (FE) servers provide the same functionality as in Lync 2010. The main role of the FE servers is to provide user authentication, registration, presence, IM, web conferencing, and application sharing functionalities. FE servers also provide an address book service and distribution list expansion. FE servers are provisioned in a front-end pool and are configured identically to provide scalability and failover capability to Lync end-users. In order to load balance the FE servers, it is required that the topology contain two or more FE servers.

In Lync 2013, the Microsoft Lync Director role has been incorporated directly into the FE server instead of having a separate instance of a virtual machine or a server. The FE Servers are used as registrars for all authentication requests.

Active Directory Domain Services (AD DS)

All Lync servers referenced within the topology, with the exception of the Edge Servers, must be joined by a domain and in Active Directory Domain Services (AD DS). Lync users are managed within the AD Domain and Lync Communication Server Control Panel (CSCP). The AD DS is required in a Lync 2013 topology.

Back End (BE) Server

The Back End (BE) servers run Microsoft SQL and provide database services for the front-end pool. The information stored in the SQL servers includes user contact lists, presence information, conferencing details, and conferencing schedule information. The SQL server can be configured as a single back-end server; however, a cluster of two or more servers is recommended for failover. The BE server requirement can be implemented with SQL 2008.

Edge Server

The edge server enables external users to communicate and collaborate with internal users. Multiple edge servers can be deployed in a pool for redundancy. The edge server also enables connectivity to third-party IM services such as Windows Live, AOL and Yahoo.

AV Conferencing Server

The Audio/Visual (AV) Conferencing Server provides AV conferencing functionalities for the Lync solution In the Lync Server 2013 topology it is embedded on the Front End server unless large scale conference capability is required.

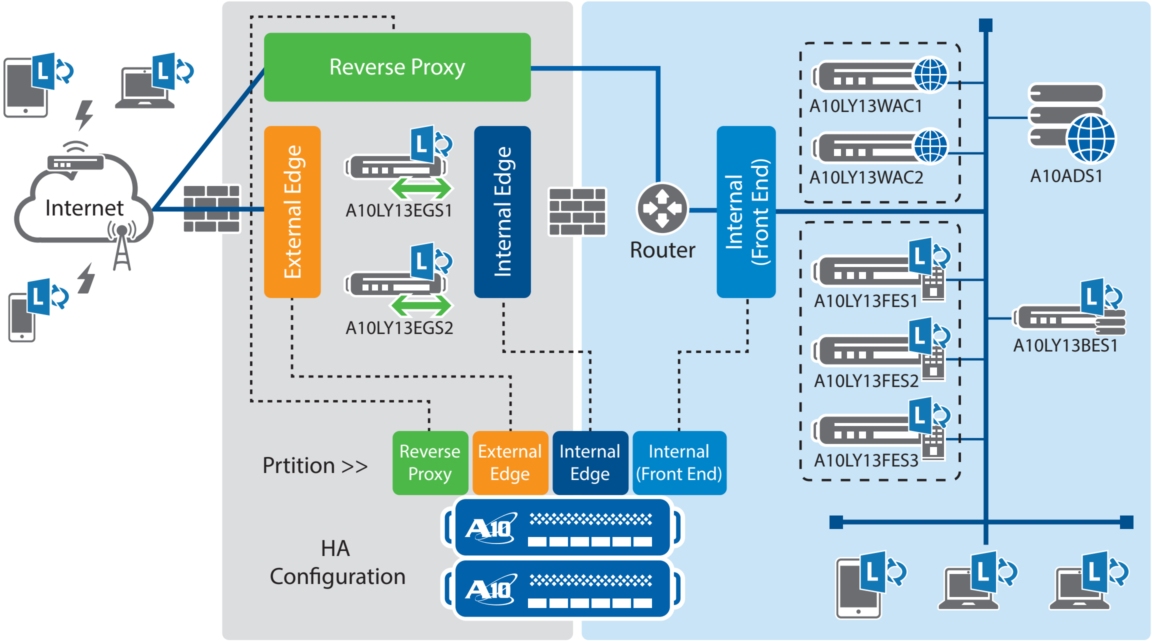


Figure 1: Lab topology

Note: ADP: Application Delivery Partition is a standard feature to support multiple partitions on a single Thunder ADC product.

Role	VIP	Hostname	IP address
AD, Internal CA, Internal DNS	NA	A10ADDS	192.168.10.14/24
Front End	192.168.10.80/24	LYNC13FES1	192.168.10.17/24
		LYNC13FES2	192.168.10.18/24
		LYNC13FES3	192.168.10.19/24
Back End	NA	LY13BES1	192.168.10.20/24
External Edge	172.17.0.111, 112, 113/24	LY13EGS1	172.17.0.21, 22, 23/24
		LY13EGS2	172.17.0.31, 32, 33/24
Internal Edge	172.19.0.101/24	LY13EGS1	172.19.0.121/24
		LY13EGS2	172.19.0.131/24
Office Web Apps	192.168.10.86/24	LY13WAC1	192.168.10.23/24
		LY13WAC2	192.168.10.24/24

Note: CA: Certificate Authority

1.2 Deployment Guide Notes:

1. A10 Thunder ADC appliances running A10 Networks' Advanced Core Operating System (ACOS®) version 2.7.1-P3, configured with ADPs enabled for Layer 3 Virtualization (L3V). The solution can also be deployed with non-L3V and will require at least 3 ACOS physical or virtual devices.
2. The lab Thunder ADC setup was configured using a one-arm deployment for easy deployment and testing.
3. If you deploy the feature called Explicit HTTP Proxy, you must deploy 2.7.2 P2 or later code for feature supportability.
4. The Microsoft Lync 2013 Server was tested through communication with Voice, IM, Presence, Desktop Collaboration and Audio Video (AV) conferencing. Testing was performed for both internal and external users.
5. Testing was performed using Microsoft Lync Server 2013 Enterprise Edition Server with 64-bit Microsoft SQL Server 2012 Enterprise Edition Version 11.00.2100.60.
6. All Lync 2013 Server components were running on Windows 2012 (64-bit) Standard Edition Server.
7. Lync 2013 Unified Client 64-bit on Windows 7 and Lync 2013 for iPhone 5.1 was used for mobile client.
8. Office Web Apps Server (WAC) was tested with Desktop Sharing, Program and Whiteboard, Poll and SharePoint presentation services/applications.

2 Configuring the Thunder ADC Device

The Thunder ADC device provides the following management interfaces:

- Command-Line Interface (CLI)

  Text-based interface in which commands are entered on a command line. The CLI is directly accessible through the serial console or over the network using either of the following protocols:

  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)

- Graphical User Interface (GUI)

  Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

  Note: *HTTP requests are redirected to HTTPS by default on the Thunder ADC device.*

By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP and HTTPS are enabled by default on the management interface only, and disabled by default on all data interfaces.

2.1 Log into the CLI

The Thunder ADC provides advanced features for securing management access to the device. This section assumes that only the basic security settings are in place.

To log into the CLI using SSH:

1. On a PC connected to a network that can access to a dedicated management interface, open an SSH connection to the IP address of the management interface.

Note: *The default IP address is 172.31.31.31*

2. Generally, if this is the first time the SSH client has accessed the Thunder ADC, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. (Press "Enter".)
3. At the "login as:" prompt, enter the username "admin".
4. At the Password: prompt, enter the admin password. The default password is "a10". If the admin username and password are valid, the command prompt for the User EXEC level of the CLI appears:

```
ACOS>
```

The User EXEC level allows you to enter a few basic commands, including some show commands as well as ping and traceroute.

5. To access the Privileged EXEC level of the CLI and allow access to all configuration levels, enter the "enable" command. At the "Password:" prompt, enter the enable password as blank. (Then press "Enter".)

   Note: *This is not the same as the admin password, although it is possible to configure the same value for both passwords.*

   If the enable password is correct, the command prompt for the Privileged EXEC level of the CLI appears:

   ```
   Thunder#
   ```

6. To access the global configuration level, enter the "config" command. The following command prompt appears:

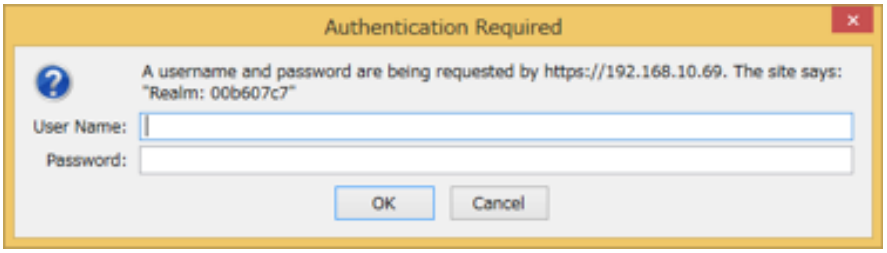
   ```
   Thunder(config)#
   ```

   Note: *See the Thunder Series Configuration Guide, or the Thunder Series System Configuration and Administration Guide and Application Delivery and Server Load Balancing Guide, for additional features and functions of the Thunder ADC device.*

2.2 Log onto the GUI

To log onto the GUI:

In your web browser, enter the HTTPS request with the management IP address of the Thunder ADC device like https://management-IP-address/. A logon dialog is displayed. The name and appearance of the dialog depends on the browser you are using.



A username and password are being requested by https://192.168.10.69. The site says: "Realm: 00b607c7"

Figure 2: GUI login dialog

Note: *Dialog name and display image are different depending on the browser and browser version used. In this test the Firefox browser is used.*

Note: *Since there is no root certificate for Thunder ADC's internal CA, which issues web server certificates for management site on access PC, warnings or alert messages are shown upon first accessing the device. When the security exception process is done, the above logging prompt will come up.*

Note: *For the default admin credentials, the username is "admin" and the password is "a10."*

Enter your admin username and password and click **OK**.

The Summary page will appear, showing at-a-glance information for your Thunder ADC device. You can access this page again at any time while using the GUI, by navigating to **Monitor > Overview > Summary**.

3 Services Required for Lync 2013 Deployment

The following tables list the services required for a Lync 2013 Enterprise Server deployment.

Table 1: Services on Front End Server

Service Name	Port	VIP Type	Source NAT	Feature Template	Usage Note
Lync Server Front-End Service	135	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.
Lync Server Web Compatibility service	443	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components). Client SSL template is required if SSL offload is configured.
Web Server Component	4443	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for Web access from remote user. Client SSL template is required if SSL offload is configured.
Lync Server Front-End Service	444	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for HTTPS communication between the Focus (the Lync Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.
Lync Server Front-End Service	5061	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: SIP 5060	Used by Standard Edition servers and Front End pools for: • All internal SIP communications between servers (MTLS) • SIP communications between Server and Client (TLS) • SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.

Table 2: Optional Services on Front End Server

Service Name	Port	VIP Type	Source NAT	Feature Template	Usage Note
Lync Server Application Sharing Service	5065	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP listening requests for application sharing.
Lync Server Response Group Service	5071	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP requests for the Response Group application.
Lync Server Conferencing Attendant Service (Dial-in Conferencing)	5072	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP requests for Attendant (dial in conferencing).
Lync Server Conferencing Announcement Service	5073	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing).
Lync Server Call Park Service	5075	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP requests for the Call Park application.
Lync Server Audio Test Service	5076	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Used for incoming SIP requests for the Audio Test service.

Note: *Details of port and protocol Lync Front-End Server uses are described in the following URL:* http://technet.microsoft.com/en-us/library/gg398833.aspx

Table 3: Services on Internal Edge

Role/Protocol	Port	VIP Type	Source NAT	Feature Template	Usage Note
STUN/MSTURN	443	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Fallback path for A/V media transfer between internal and external users if UDP communication cannot be established. TCP is used for file transfer and desktop sharing.
STUN/MSTURN	3478	UDP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Preferred path for A/V media transfer between internal and external users.
Access/SIP	5061	TCP/ MTLS	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Inbound/Outbound SIP traffic (to/from Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address) from/to Edge Server internal interface.
SIP/MTLS	5062	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server.

Note: *Details of port and protocol Lync Edge Server uses are described in the following URL:* http://technet.microsoft.com/en-us/library/gg398739.aspx

Table 4: Services on External Edge

Role/Protocol	Port	VIP Type	Source NAT	Feature Template	Usage Note
Access/ SIP(TLS)	443	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Client-to-server SIP traffic for external user access
Access/ SIP(MTLS)	5061	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	SIP signaling, federated and public IM connectivity using SIP
Web Conferencing /PSOM(TLS)	443	TCP	Yes	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	Web Conferencing media
A/V / STUN,MSTURN	443	TCP	-	Persistence: SIP TCP: TCP Health Monitor: Lync-HM	STUN/TURN negotiation of candidates over TCP/443
A/V / STUN,MSTURN	3478	UDP	-	Persistence: SIP Health Monitor: Lync-HM	STUN/TURN negotiation of candidates over UDP/3478

Note: During feature selection (Figure 4) of the external edge pool installation, you will be asked to deploy the Lync edge server pool with either single or multiple FQDNs and IP addresses. Deselecting the "use a single FQDN and IP address" option will enable the external edge pool to have multiple IP configurations. The Thunder ADC device can be deployed in either a single IP configuration or a multiple IP configuration. In a multiple IP configuration, three public "virtual" IP addresses (VIPs) will be required for Access, WebConf and AV. For a single FQDN and IP address configuration, one public VIP will be required.

Protocol Definition

DCOM - Distributed Component Object Model

FQDN - Fully Qualified Domain Name

MTLS - Multiplexed Transport Layer Security

PSOM - Persistent Shared Object Model

STUN - Session Traversal Utilities for NAT

SIP - Session Initiation Protocol

TLS - Transport Layer Security

TURN - Traversal Using Relay NAT

Table 5: Service on Office Web Apps Server (Option)

Service Name	Port	VIP Type	Source NAT	Feature Template	Usage Note
Office Web Apps Server Service	443	TCP	Yes	Persistence: Cookie TCP: TCP Health Monitor: WAC-80 Client SSL template: Required	Used for PowerPoint content sharing to Lync 2013 clients. Lync Server components is still used for Lync 2010 client. SSL Offload is recommended.

Table 6: Services on Reverse Proxy (Option)

Service Name	Port	VIP Type	Source NAT	Feature Template	Usage Note
Lync Server Published Web Service	443 >> 4443 (redirect)	TCP	Auto	Persistence: Cookie TCP: TCP Health Monitor: Lync-HM Client SSL template: Required Server SSL Template: Required aFleX® or HTTP Template: Required[1]	Used for communication to Lync Front-End Web service from remote user. Traffic sent to port 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic.
Office Web Apps Published Service	443	TCP	Auto	Persistence: Cookie TCP: TCP Health Monitor: Lync-HM Client SSL template: Required Server SSL Template: Required aFleX or HTTP Template: Required[1]	Used for PowerPoint content sharing/shared from remote user.

Note: *Details of ports and protocol of reverse proxy is described at the following URL:* http://technet.microsoft.com/en-us/library/jj204932.aspx

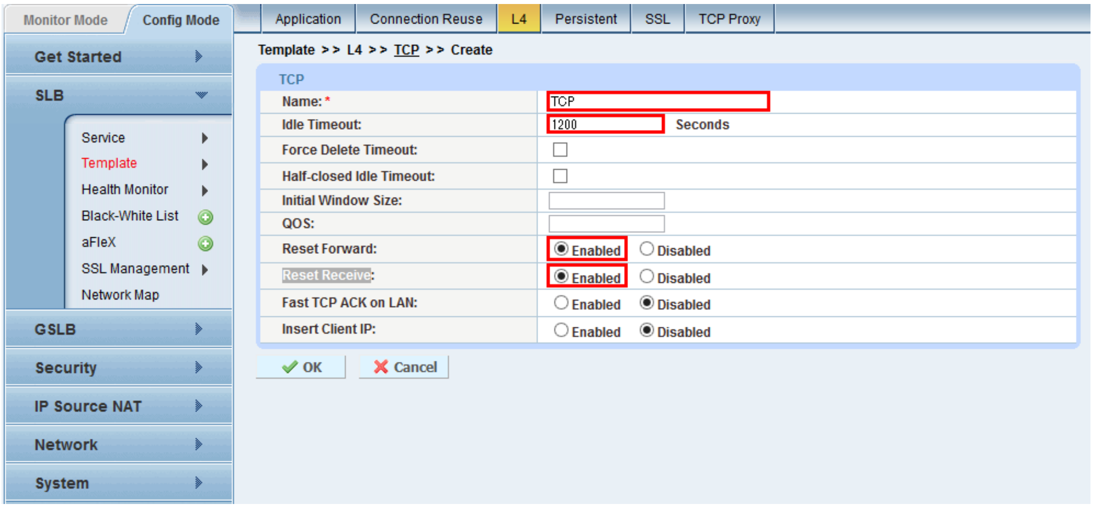
3.1 Feature Template and Configuration Template on Thunder ADC

The template and configuration below are used for a specific server role. Please refer to *Services Required for Lync 2013 Deployment* to find out where/how to use it.

A. How to Create a TCP Template

1. Move to Config Mode > SLB > Template > L4.
2. Click Add and configure below.
   a. Name: **TCP**
   b. Idle Timeout: **1200**
   c. Reset Forward: **Enabled**
   d. Reset Receive: **Enabled**
3. Click **OK** after configuration is completed and click **Save** to save configuration.

[1] An aFleX or HTTP Template is required to handle URI-based service selection with a single published IP address.



Template >> L4 >> TCP >> Create

TCP

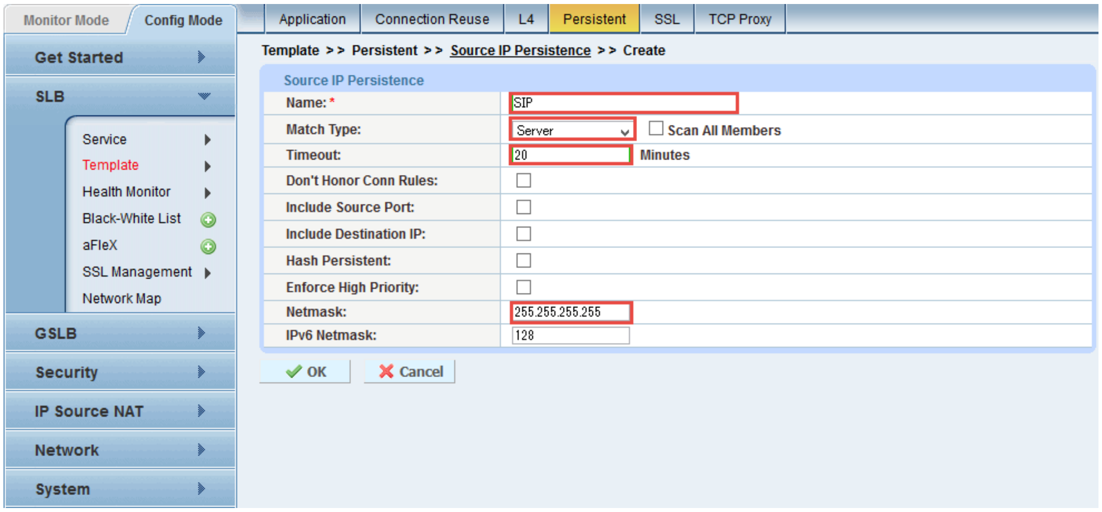
Name: *	TCP
Idle Timeout:	1200 Seconds
Force Delete Timeout:	□
Half-closed Idle Timeout:	□
Initial Window Size:	
QOS:	
Reset Forward:	● Enabled ○ Disabled
Reset Receive:	● Enabled ○ Disabled
Fast TCP ACK on LAN:	○ Enabled ● Disabled
Insert Client IP:	○ Enabled ● Disabled

Figure 3: L4 TCP template

Note: The Idle Timeout value is the timer that resets an idle TCP connection on the Thunder ADC device.

B. How to Configure Source IP Persistence

1. Move to Config Mode > SLB > Template > Persistent > Source IP Persistence.
2. Click Add and configure below.
   a. Name: SIP (used for Lync load balancing and RP is used for reverse proxy)
   b. Match Type: Server
   c. Timeout: 20 Minutes
   d. Netmask: 255.255.255.255 (default value)
3. Click OK after configuration is completed and click Save to save the configuration.



Template >> Persistent >> Source IP Persistence >> Create

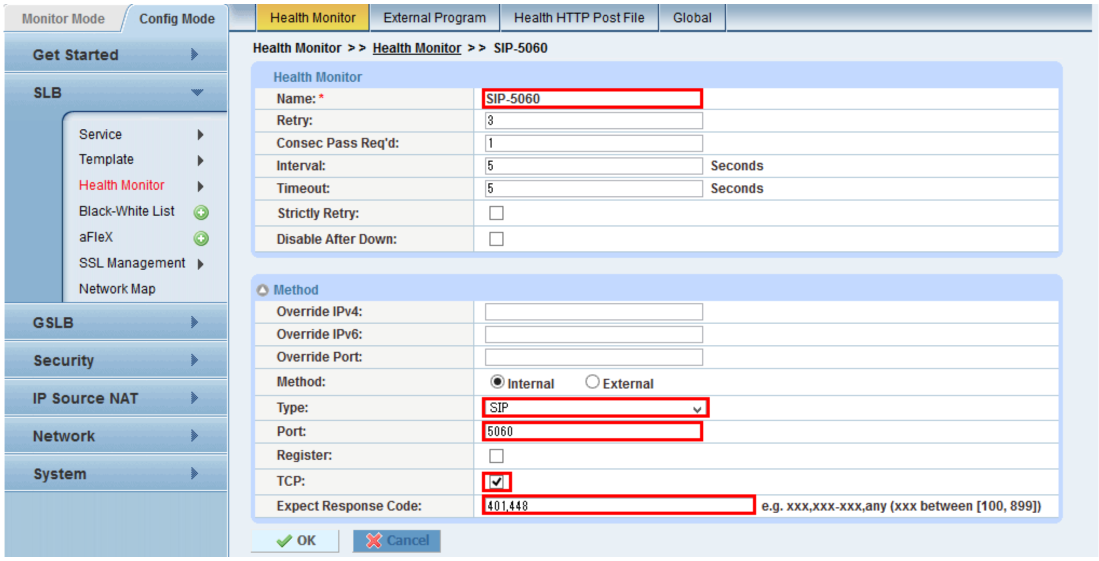
Source IP Persistence

Name: *	SIP
Match Type:	Server □ Scan All Members
Timeout:	20 Minutes
Don't Honor Conn Rules:	□
Include Source Port:	□
Include Destination IP:	□
Hash Persistent:	□
Enforce High Priority:	□
Netmask:	255.255.255.255
IPv6 Netmask:	128

Figure 4: Source IP persistence template

C. How to Configure a Health Monitor

1. Move to Config Mode > SLB > Health Monitor > Health Monitor.
2. Click Add and configure below.
   a. Name: Lync-HM
   b. Use the default value in other fields
3. Click OK after completion and click Save to save the configuration data into memory if needed.
4. Follow the same procedure to configure a Health Monitor for Lync SIP signaling as below.
   a. Name: SIP-5060
   b. Type: SIP
   c. Port: 5060
   d. TCP: check
   e. Expected Response Code: 401,488
5. Click OK after configuration is completed and click Save to save the configuration.



Health Monitor >> Health Monitor >> SIP-5060

Health Monitor

Name: *	SIP-5060
Retry:	3
Consec Pass Req'd:	1
Interval:	5 Seconds
Timeout:	5 Seconds
Strictly Retry:	□
Disable After Down:	□

Method

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	● Internal ○ External
Type:	SIP
Port:	5060
Register:	□
TCP:	☑
Expect Response Code:	401,448 e.g. xxx,xxx-xxx,any (xxx between [100, 899])

Figure 5: Health Monitor configuration

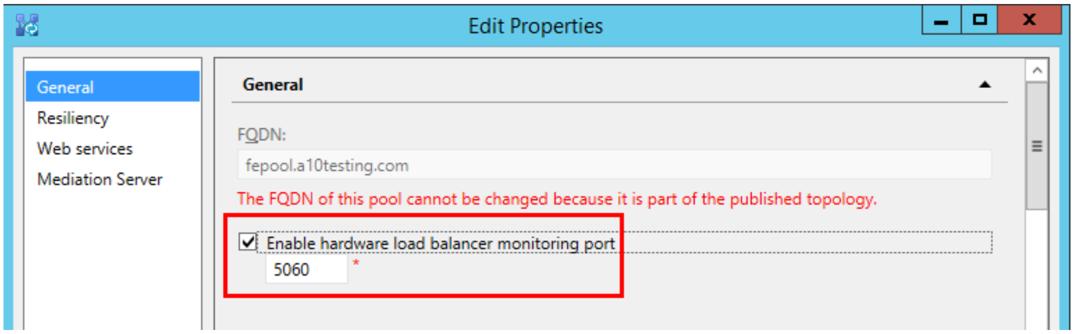
Note: You can configure a TCP port base health check. If you want to use it, you have to configure a health monitor configuration for all used TCP ports. The following is a sample configuration:

a. Name: TCP-443
b. Interval: 30
c. Timeout: 10
d. Type: TCP
e. Port: 443
f. HalfOpen: False

3.2 How to Enable Hardware Load Balancer Monitoring Port on Lync Front-End Server

This configuration is enabled on Lync Server 2013 Enterprise Edition Front-End Pool in Lync Server 2013 Topology Builder. If it is enabled, the Thunder ADC can monitor Lync Server 2013 Front End Server through TCP port 5060.

1. Start the Lync Topology Builder on one of Lync Front End servers.
2. Chose "Download Topology from existing deployment" and save the current topology as a file into an appropriate location, such as a local folder. If it is the first time using the topology builder in Lync Server Front End pool, you should select New Topology.
3. Move to Lync Server 2013 > Site (defined before) > Lync Server 2013 > Enterprise Edition Front End pools.
4. In this test environment, the properties of the Lync2013.a10domain.a10.local pool are being modified. Check "Enable hardware load balancer monitoring port" and enter "5060" into the column as below.

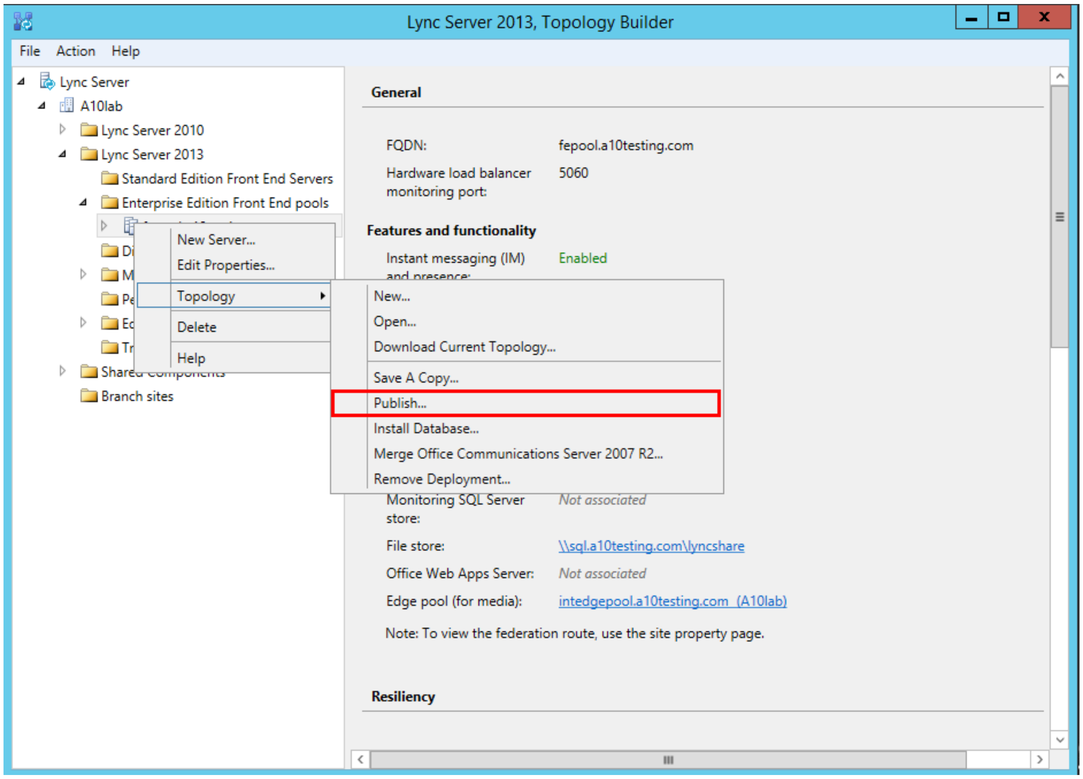


FQDN:
fepool.a10testing.com
The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable hardware load balancer monitoring port
5060 *

Figure 6: Enable hardware load balancer monitoring port on Lync Server Topology

5. Chose pool name, right click on it, and move to Topology > Publish to reflect the modified topology into the database.



FQDN: fepool.a10testing.com
Hardware load balancer monitoring port: 5060
Instant messaging (IM) and presence: Enabled
Monitoring SQL Server store: Not associated
File store: \\sql.a10testing.com\lyncshare
Office Web Apps Server: Not associated
Edge pool (for media): intedgepool.a10testing.com (A10lab)
Note: To view the federation route, use the site property page.

Figure 7: Publish modified topology

Note: Publish is required to enable modified topology.

4 Load Balancing for Lync Front End Pool

One or more pools can be configured in each site and one or more Lync Front End Servers can be configured in each pool. The Lync Front End Server pool is a core component and composed of one or more Lync Front End Servers. IM/Presence, every Conference service, collaboration, voice, and more services are provided by Lync Front End pool. If there are multiple Lync Front End Servers in a pool, and one of them is under service outage mode, the rest of the healthy Front End Servers continue to provide all services to the end user.

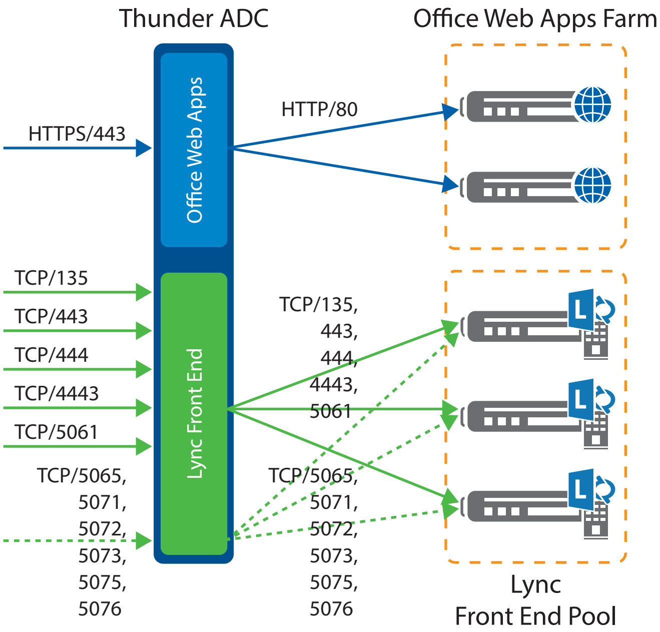


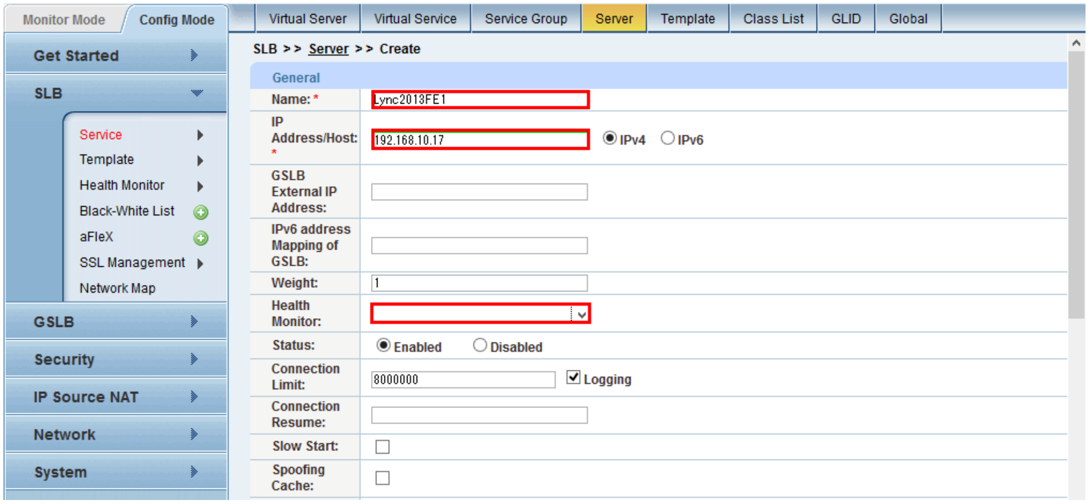
Figure 8: Load balancing image diagram for Front End pool and Office Web Apps

The following section describes how to configure a redundant Lync Server Front End Enterprise pool (services) on the Thunder ADC.

4.1 Server Configuration

Configure Lync Front End Servers on the Thunder ADC.

1. Move to **Config Mode** > **SLB** > **Service** > **Server**.
2. Click **Add** to create a new server.
3. In this test environment the following information is used:
   a. Name: **Lync2013FE1**
   b. IP Address/Host: **192.168.10.17**
   c. Health Monitor: leave blank (Health Monitor is configured at Service group)



SLB >> Server >> Create

General

Name: *	Lync2013FE1
IP Address/Host: *	192.168.10.17 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□

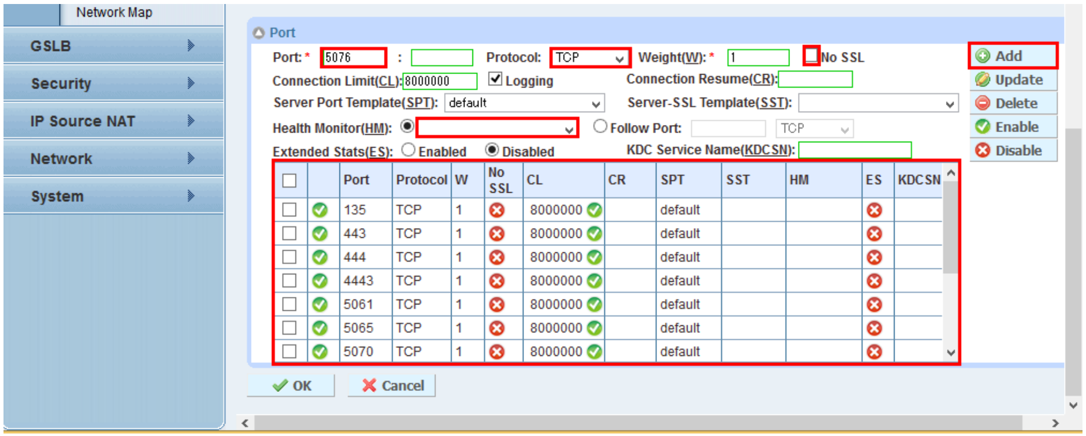
Figure 9: Configure a Lync Front End Server

4. Add port information on the last half of this page.

   a. Enter the port number, select a proper protocol type, choose blank in Health Monitor (HM), and click **Add**.

   b. Repeat the above procedure for all required ports. Refer to Table 1 and Table 2 to clarify which ports should be configured.

Note: *Check "No SSL" if configured port does not use SSL.*



Port

Port: * 5076 : Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Server-SSL Template(SST):

Health Monitor(HM): ● ○ Follow Port: TCP

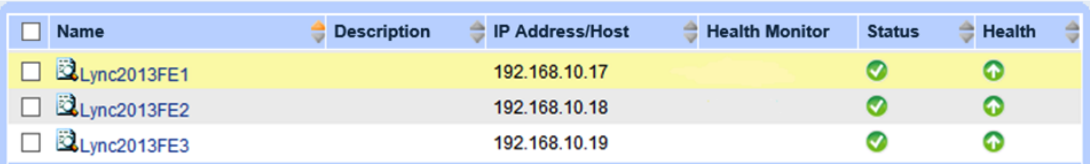
Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	135	TCP	1	☒	8000000 ✓		default			☒	
□	✓	443	TCP	1	☒	8000000 ✓		default			☒	
□	✓	444	TCP	1	☒	8000000 ✓		default			☒	
□	✓	4443	TCP	1	☒	8000000 ✓		default			☒	
□	✓	5061	TCP	1	☒	8000000 ✓		default			☒	
□	✓	5065	TCP	1	☒	8000000 ✓		default			☒	
□	✓	5070	TCP	1	☒	8000000 ✓		default			☒	

Figure 10: Configure ports for Lync Front End Server

5. Click **OK** after the configuration is done and click **Save** to save the configuration.

6. Repeat the above steps (from Step 2 to Step 4) until all Front End Servers' configurations are completed. In this guide, additionally both A10LY13FES2 and A10LY13FES3 are configured.



□	Name	Description	IP Address/Host	Health Monitor	Status	Health
□	Lync2013FE1		192.168.10.17		✓	↑
□	Lync2013FE2		192.168.10.18		✓	↑
□	Lync2013FE3		192.168.10.19		✓	↑

Figure 11: Configured Lync Front End Server list on the Thunder ADC

4.2 Service Group Configuration

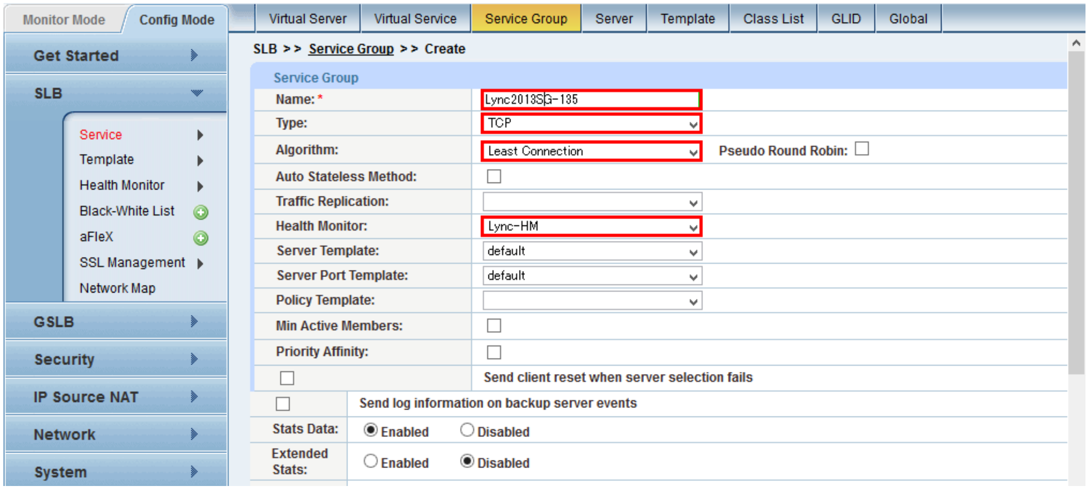
Configure a Service Group for Lync Front End Servers next.

1. Move to Config Mode > SLB > Service > Service Group.
2. Click Add and create a new service group for Lync Front End Servers.
3. In this test environment the following data is used:
   a. Name: Lync2013SG-135

   b. Type: TCP

   c. Algorithm: Least Connection

   d. Health Monitor: Lync-HM



SLB >> Service Group >> Create

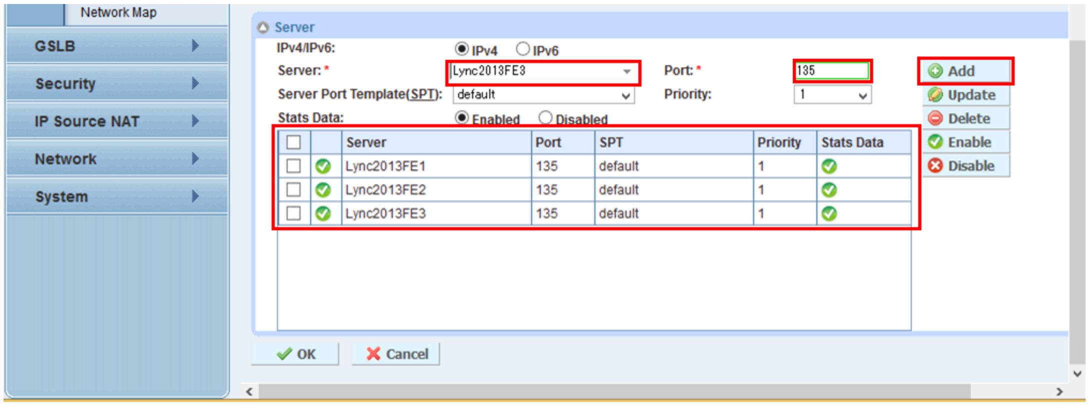
Service Group

Name: *	Lync2013SG-135
Type:	TCP
Algorithm:	Least Connection — Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	Lync-HM
Server Template:	default
Server Port Template:	default
Policy Template:	
Min Active Members:	□
Priority Affinity:	□
□	Send client reset when server selection fails
□	Send log information on backup server events
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled

Figure 12: Lync Front End Servers Service Group configuration

Note: The set of real servers, port and server selection algorithm are defined at the Service Group level. Multiple service groups can be defined if the application uses multiple ports on a single IP.

   e. Scroll down to the Server part and add more than one server with appropriate port number.



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * Lync2013FE3 Port: * 135

Server Port Template(SPT): default Priority: 1

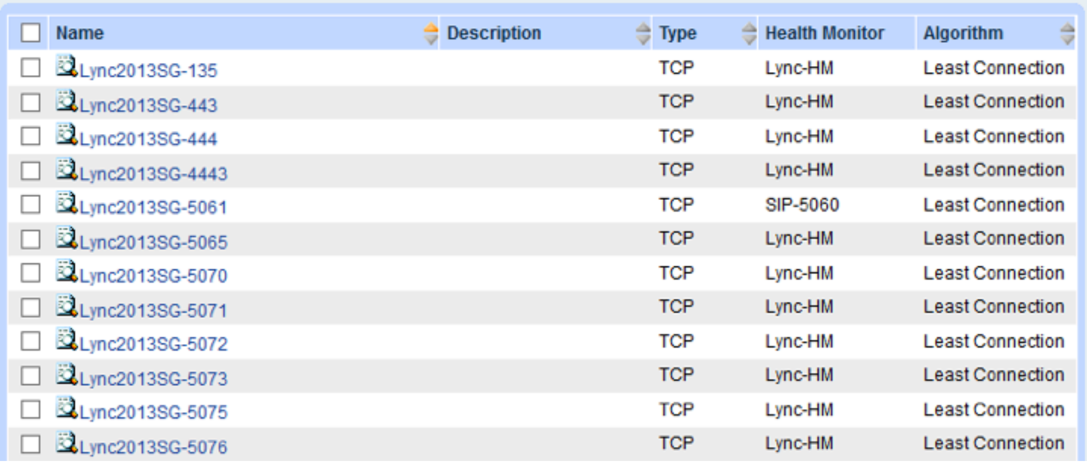
Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	Lync2013FE1	135	default	1	✓
□	✓	Lync2013FE2	135	default	1	✓
□	✓	Lync2013FE3	135	default	1	✓

Figure 13: Lync Front End Server Service Group

   f. Click OK after the configuration is done and click Save to save the configuration.

   g. Repeat the above steps (from Step a to Step e) for all required ports and optional ports if needed. Please refer to Table 1 and Table 2 to clarify what ports should be configured.



□	Name	Description	Type	Health Monitor	Algorithm
□	Lync2013SG-135		TCP	Lync-HM	Least Connection
□	Lync2013SG-443		TCP	Lync-HM	Least Connection
□	Lync2013SG-444		TCP	Lync-HM	Least Connection
□	Lync2013SG-4443		TCP	Lync-HM	Least Connection
□	Lync2013SG-5061		TCP	SIP-5060	Least Connection
□	Lync2013SG-5065		TCP	Lync-HM	Least Connection
□	Lync2013SG-5070		TCP	Lync-HM	Least Connection
□	Lync2013SG-5071		TCP	Lync-HM	Least Connection
□	Lync2013SG-5072		TCP	Lync-HM	Least Connection
□	Lync2013SG-5073		TCP	Lync-HM	Least Connection
□	Lync2013SG-5075		TCP	Lync-HM	Least Connection
□	Lync2013SG-5076		TCP	Lync-HM	Least Connection

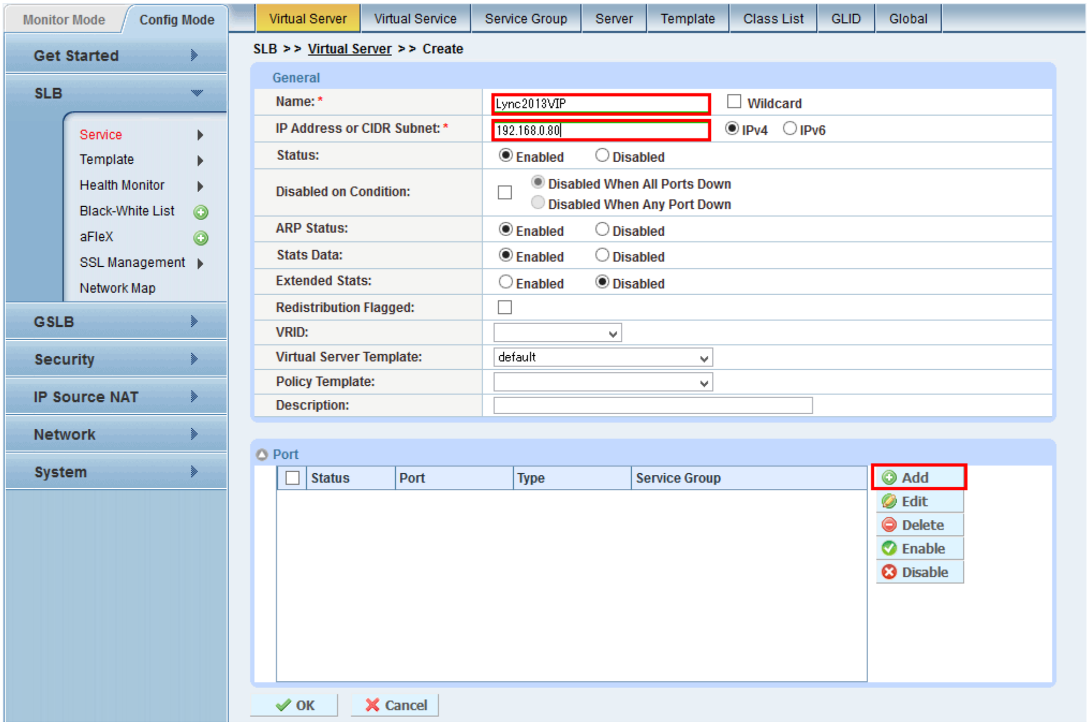
Figure 14: Lync Front End Server Service Group list

4.3 Virtual Server Configuration

Next, create a virtual server for services on Front End Server.

1. Move to Config Mode > SLB > Service > Virtual Server.
2. Click Add to create a virtual server.
3. In this test environment the following data is used:
   a. Name: Lync2013VIP
   b. IP Address or CIDR Subnet : 192.168.0.80

Note: Multiple virtual servers can be configured on the Thunder ADC. A virtual server receives access requests from a client instead of a real server. Thunder ADC chooses a proper server which is configured within the associated service group and forwards client request to it.



SLB >> Virtual Server >> Create

General

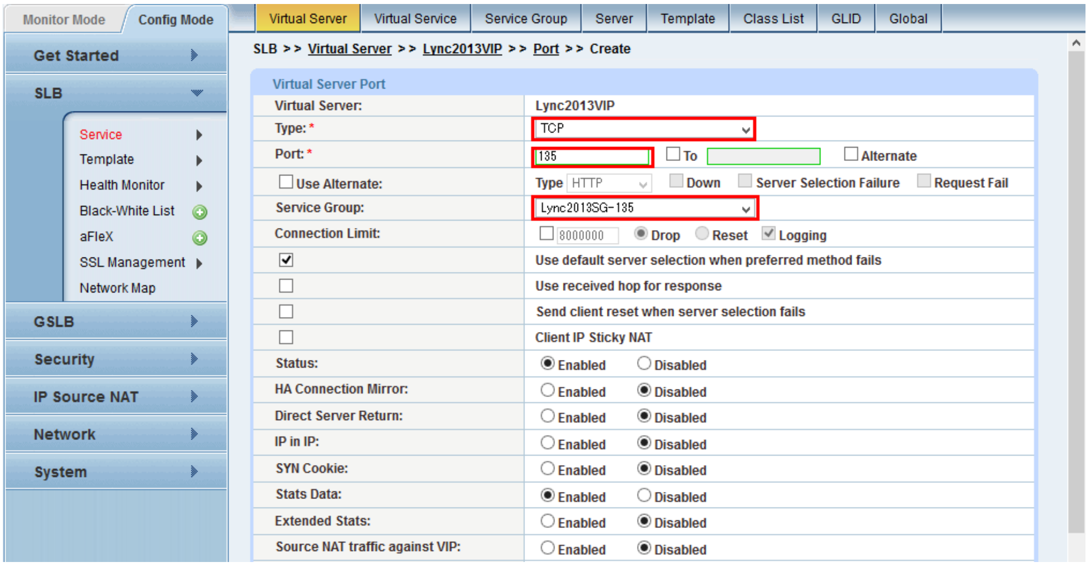
Name: *	Lync2013VIP □ Wildcard
IP Address or CIDR Subnet: *	192.168.0.80 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
VRID:	
Virtual Server Template:	default
Policy Template:	
Description:	

Port

□	Status	Port	Type	Service Group

Figure 15: Lync Front End Server virtual server configuration

4. Scroll down to the Port section and click Add to configure a virtual server port.
5. In the Virtual Server Port setting section, the test environment inputs the following configuration:
   a. Type : **TCP**
   b. Port: **135**
   c. Service Group: **Lync2013SG-135**



SLB >> Virtual Server >> Lync2013VIP >> Port >> Create

Virtual Server Port

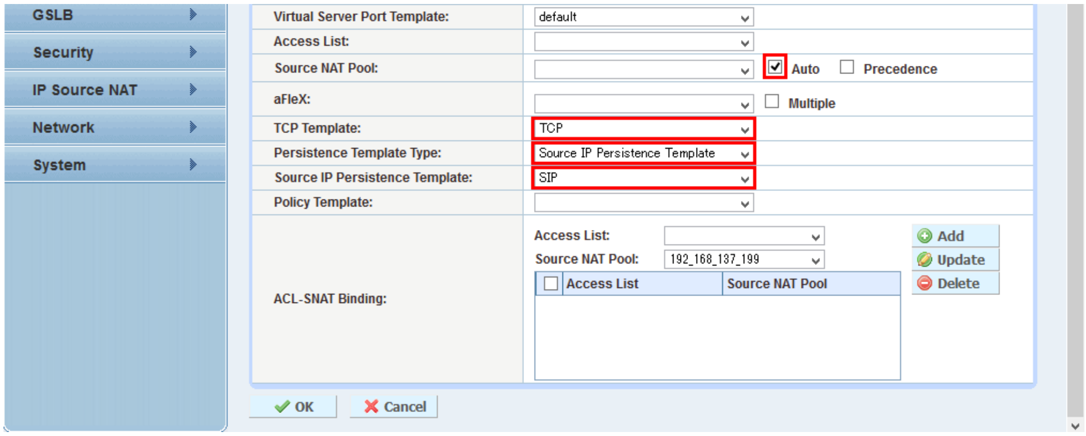
Virtual Server:	Lync2013VIP
Type: *	TCP
Port: *	135 □ To □ Alternate
□ Use Alternate:	Type HTTP □ Down □ Server Selection Failure □ Request Fail
Service Group:	Lync2013SG-135
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
HA Connection Mirror:	○ Enabled ● Disabled
Direct Server Return:	○ Enabled ● Disabled
IP in IP:	○ Enabled ● Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 16: Lync Front End Server virtual port configuration

   d. Source NAT Pool: **Auto**

Note: The original Source IP Address is replaced by an IP address of the Thunder ADC's interfaces which forcedly connects to a real server.

   e. TCP Template: **TCP**
   f. Persistence Template Type: **Source IP Persistence**
   g. Source IP Persistence Template: **SIP**



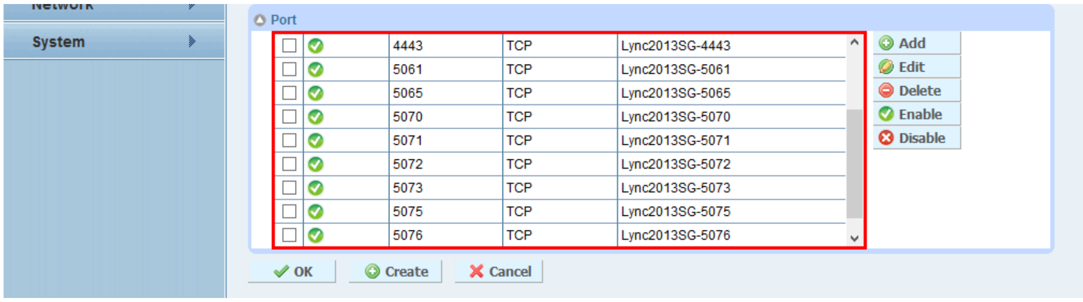
Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	☑ Auto □ Precedence
aFleX:	□ Multiple
TCP Template:	TCP
Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	SIP
Policy Template:	
ACL-SNAT Binding:	Access List: Source NAT Pool: 192_168_137_199 □ Access List | Source NAT Pool Add Update Delete

✓ OK ✗ Cancel

Figure 17: Lync Front End Server Feature template configuration

Note: The requirements of each template and of persistence are described at Services Required for Lync 2013 Deployment. Please refer to Table1 and Table 2.

6. Click **OK** after the configuration is completed and click **Save** to save the configuration.
7. Repeat the above steps (from 3 to 6) for all required and optional ports. Please refer to Table 1 and Table 2 to clarify which ports should be configured.



Network

System

Port

☐	✓	4443	TCP	Lync2013SG-4443
☐	✓	5061	TCP	Lync2013SG-5061
☐	✓	5065	TCP	Lync2013SG-5065
☐	✓	5070	TCP	Lync2013SG-5070
☐	✓	5071	TCP	Lync2013SG-5071
☐	✓	5072	TCP	Lync2013SG-5072
☐	✓	5073	TCP	Lync2013SG-5073
☐	✓	5075	TCP	Lync2013SG-5075
☐	✓	5076	TCP	Lync2013SG-5076

Figure 18: Virtual server port list for Lync Front End Server pool

8. Click **OK** in the virtual server configuration section after configuration of all virtual server ports are completed and click **Save** to save the configuration.

5 External Edge Load Balancing

Lync Edge server allows remote users to access internal Lync Front End Server resources through the enterprise firewall and the DMZ/perimeter network. Remote users can use Lync full functionalities, including IM/Presence, Conference, Collaboration and Enterprise Voice without a VPN connection if the Lync Edge pool is deployed. It also supports public IM connectivities, such as Skype, Yahoo and AOL, as well as federation connectivity to other companies. Lync Edge pool can be deployed with either a single Edge server or multiple Edge servers. For redundancy purposes, load balancing is required in order to deploy multiple Edge servers.

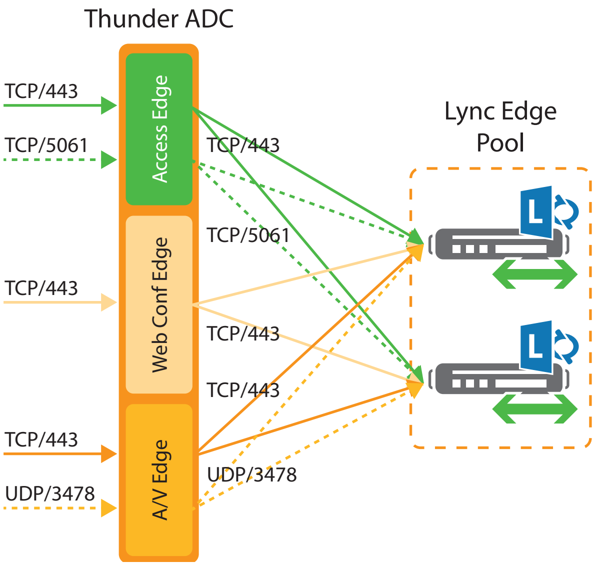


Figure 19: Load balancing image diagram for (external) Lync Edge pool

This section describes how to configure external Lync Edge pool (services) on Thunder ADC.

5.1 Server Configuration

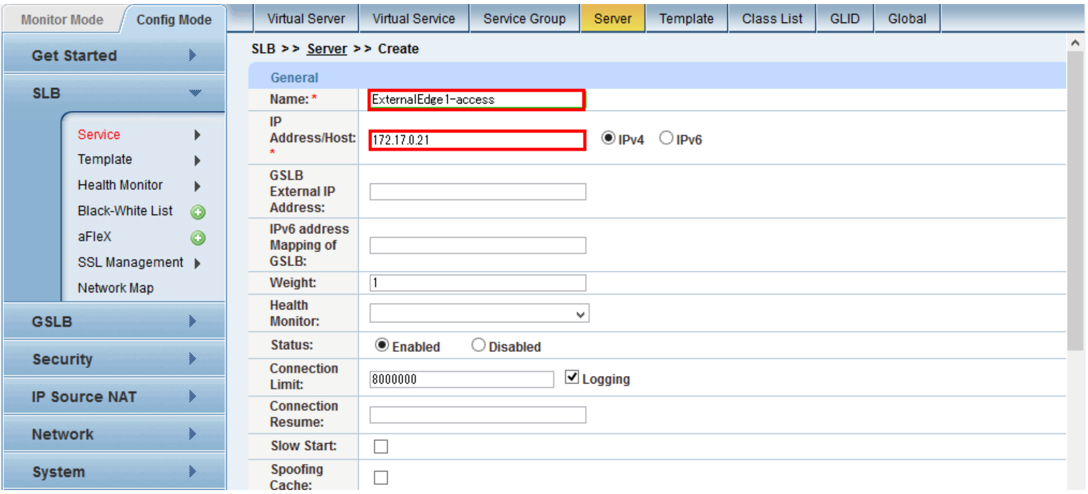
Configure a Lync External Edge Servers on the Thunder ADC.

1. Move to **Config Mode** > **SLB** > **Service** > **Server**.
2. Click **Add** to create a new server.
3. In this test environment the following input is used:

   a. Name: **ExternalEdge1-access**

   b. IP Address/Host: **172.17.0.21**

   c. Health Monitor: leave blank (Health Monitor is configured on a Service group)



SLB >> Server >> Create

General

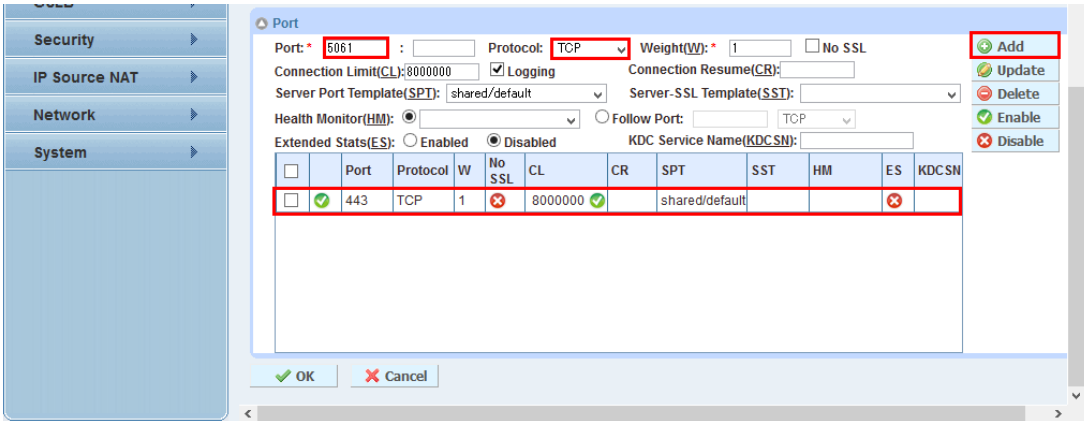
Name: *	ExternalEdge1-access
IP Address/Host: *	172.17.0.21 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□

Figure 20: External Lync Edge Server configuration

4. Scroll down to the Port section and enter an appropriate port number, select a proper protocol type, choose blank in Health Monitor (HM), and click **Add**.

   Please refer to Table 4 to clarify what port number should be configured in your environment.

5. Click **OK** after the configuration is completed and click **Save** to save the configuration.



Port

Port: * 5061 : Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): shared/default Server-SSL Template(SST):

Health Monitor(HM): ● ○ Follow Port: TCP

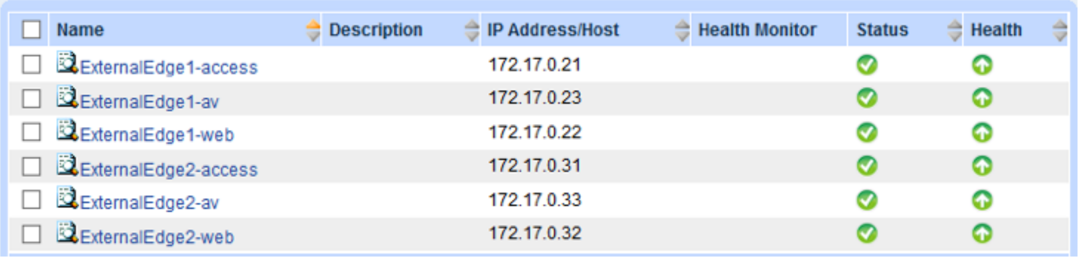
Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	443	TCP	1	☒	8000000 ✓		shared/default			☒	

Figure 21: External Lync Edge Server port configuration

Note: To confirm required ports for the external Lync Edge Server, please refer to Table 4. In this test environment, use 443/TCP for all Edge services (Access, Web Conf, A/V) and 3478/UDP for A/V Edge since individual IP addresses are assigned to each service.

6. Repeat the above steps (from 1 to 4) for all required servers. In this test environment, Web Conf and A/V for A10LY13EGS1 and all edge roles for A10LY13EGS2 are added.



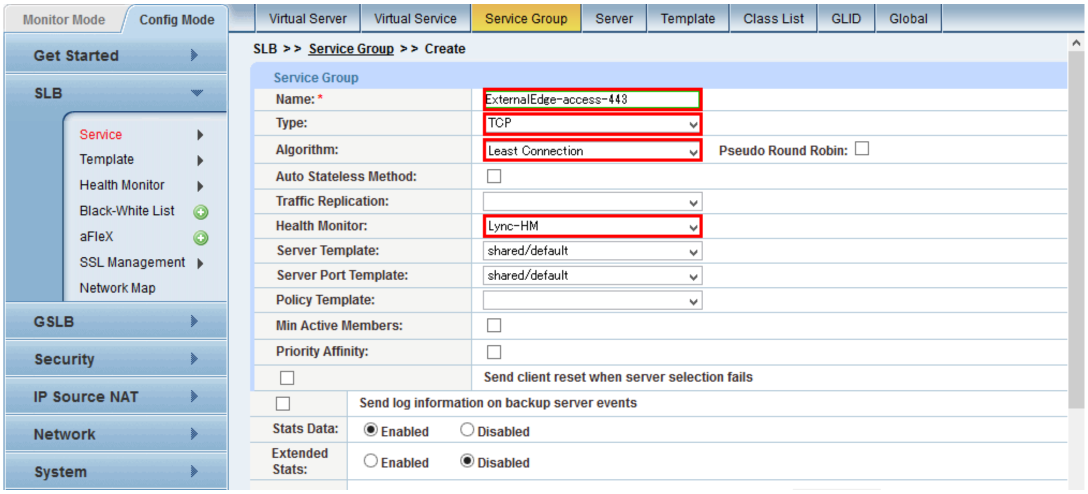
□	Name	Description	IP Address/Host	Health Monitor	Status	Health
□	ExternalEdge1-access		172.17.0.21		✓	↑
□	ExternalEdge1-av		172.17.0.23		✓	↑
□	ExternalEdge1-web		172.17.0.22		✓	↑
□	ExternalEdge2-access		172.17.0.31		✓	↑
□	ExternalEdge2-av		172.17.0.33		✓	↑
□	ExternalEdge2-web		172.17.0.32		✓	↑

Figure 22: External Edge Server list

5.2 Service Group Configuration

Next, create a service group for External Edge Servers on the Thunder ADC.

1. Move to Config Mode > SLB > Service > Service Group.
2. Click Add and create a new service group.
3. In this test environment the following input is used:
   a. Name: ExternalEdge-access-443
   b. Type: TCP
   c. Algorithm: Least Connection
   d. Health Monitor: Lync-HM



SLB >> Service Group >> Create

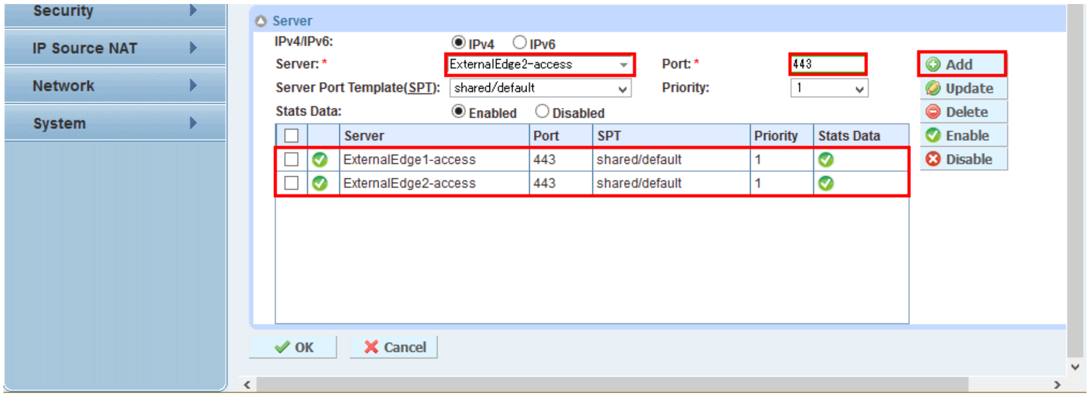
Service Group

Name: *	ExternalEdge-access-443
Type:	TCP
Algorithm:	Least Connection Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	Lync-HM
Server Template:	shared/default
Server Port Template:	shared/default
Policy Template:	
Min Active Members:	□
Priority Affinity:	□
□	Send client reset when server selection fails
□	Send log information on backup server events
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled

Figure 23: External Lync Edge Server service group configuration

Note: The set of real server, port and server selection algorithm are defined in the service group. Multiple service groups can be defined if an application uses multiple ports on single IP.

4. Scroll down to the Server section and add more than one server with the appropriate port.



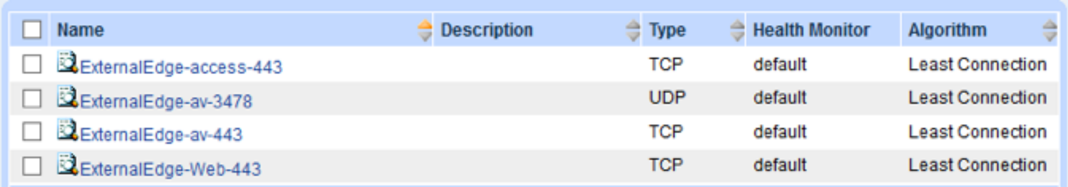
Server

IPv4/IPv6: ● IPv4 ○ IPv6
Server: * ExternalEdge2-access Port: * 443
Server Port Template(SPT): shared/default Priority: 1
Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	ExternalEdge1-access	443	shared/default	1	✓
□	✓	ExternalEdge2-access	443	shared/default	1	✓

Figure 24: Server list on the External Lync Edge service group

5. Click OK after the configuration is completed and click Save to save the configuration.
6. Repeat the above steps (from 1 to 4) for all required service groups with appropriate ports. Please refer to Table 4 to clarify what data should be configured.



☐	Name	Description	Type	Health Monitor	Algorithm
☐	ExternalEdge-access-443		TCP	default	Least Connection
☐	ExternalEdge-av-3478		UDP	default	Least Connection
☐	ExternalEdge-av-443		TCP	default	Least Connection
☐	ExternalEdge-Web-443		TCP	default	Least Connection

Figure 25: Service group list of External Lync Edge server

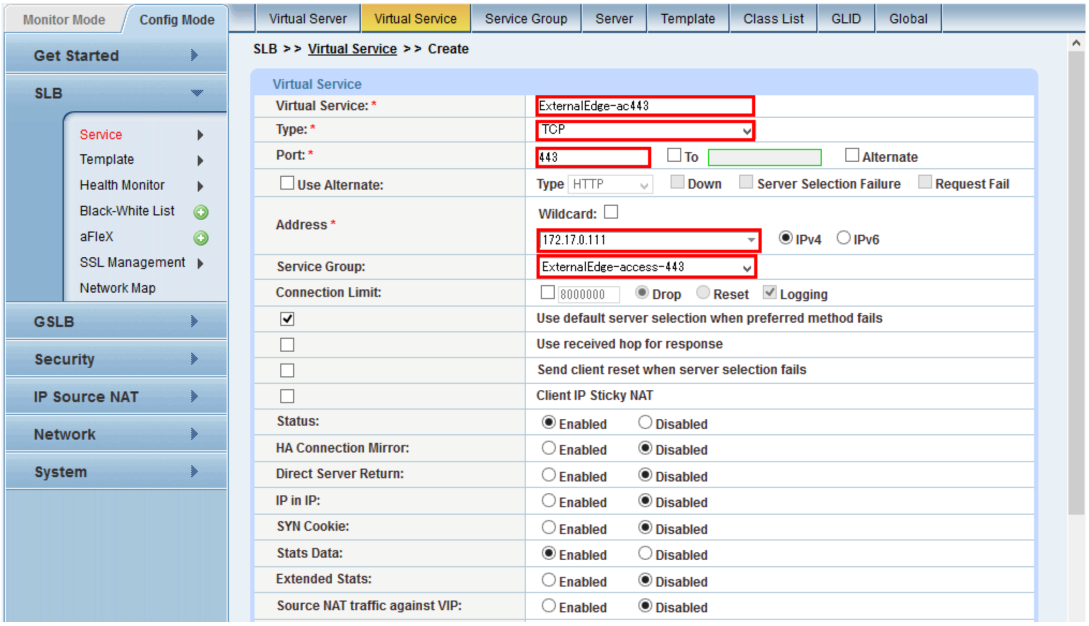
Note: *TCP/5061 for Access Edge is not configured in this environment because there is no federation and public IM connectivity configuration.*

5.3 Virtual Service Configuration

In previous Lync Front End Server load balancing settings, virtual service (virtual server port) was set up through virtual server configuration page. In this section, both the virtual service and the virtual server are configured within the virtual service configuration page. It is different from the Lync Front End Server load balancing configuration, but either configuration is supported.

In this test environment, the IP Address for each Edge role is independent, so the following steps need to be done for Web Conf, A/V Edge as well:

1. Move to **Config Mode** > **SLB** > **Service** > **Virtual Service**.
2. Click **Add** and create a virtual service.
3. In this test environment the following input is used:
   a. Virtual Service: **ExternalEdge-ac443**
   b. Type: **TCP**
   c. Port: **443**
   d. Address: **172.17.0.111**
   e. Service Group: **ExternalEdge-access-443**



SLB >> Virtual Service >> Create

Virtual Service

Virtual Service: *	ExternalEdge-ac443
Type: *	TCP
Port: *	443 ☐ To ☐ Alternate
☐ Use Alternate:	Type HTTP ☐ Down ☐ Server Selection Failure ☐ Request Fail
Address *	Wildcard: ☐ 172.17.0.111 ● IPv4 ○ IPv6
Service Group:	ExternalEdge-access-443
Connection Limit:	☐ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
☐	Use received hop for response
☐	Send client reset when server selection fails
☐	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
HA Connection Mirror:	○ Enabled ● Disabled
Direct Server Return:	○ Enabled ● Disabled
IP in IP:	○ Enabled ● Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 26: Virtual service configuration for external Lync Access Edge

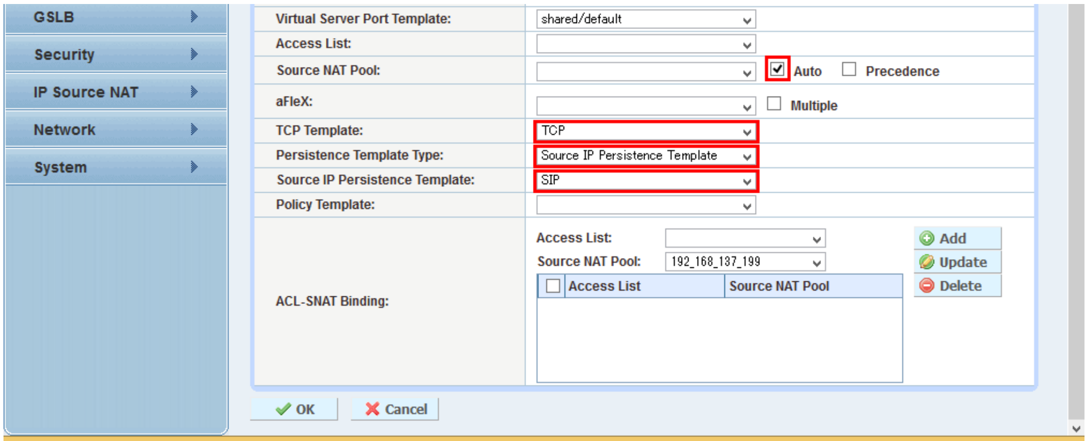
Set the following data as a feature template:

f. Source NAT Pool: **Auto**

g. TCP Template: **TCP**

h. Persistence Template Type: **Source IP Persistence Template**

i. Source IP Persistence Template: **SIP**

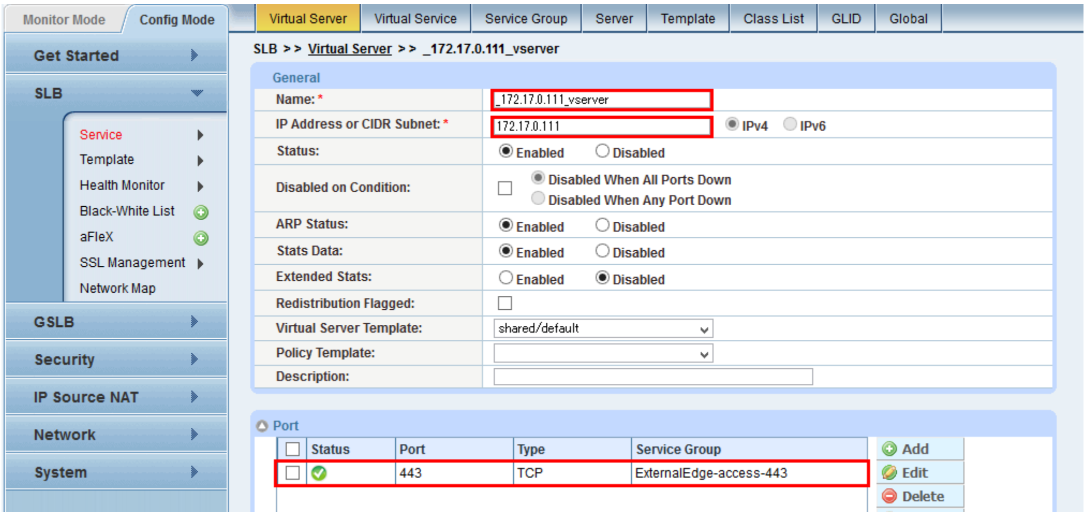


Virtual Server Port Template:	shared/default
Access List:	
Source NAT Pool:	☑ Auto □ Precedence
aFleX:	□ Multiple
TCP Template:	TCP
Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	SIP
Policy Template:	
ACL-SNAT Binding:	Access List: Source NAT Pool: 192_168_137_199 □ Access List / Source NAT Pool

Figure 27: Virtual service feature template for external Lync Access Edge pool

Note: Please refer to Table 4 to clarify what feature template and persistence should be configured.

4. Click **OK** after the configuration is completed and then click **Save** to save the configuration.
5. Repeat the above steps (from Step 1 to Step 3) for Web Conf Edge TCP/443 and A/V Edge TCP/443, UDP/3478 based on Table.4.



SLB >> Virtual Server >> _172.17.0.111_vserver

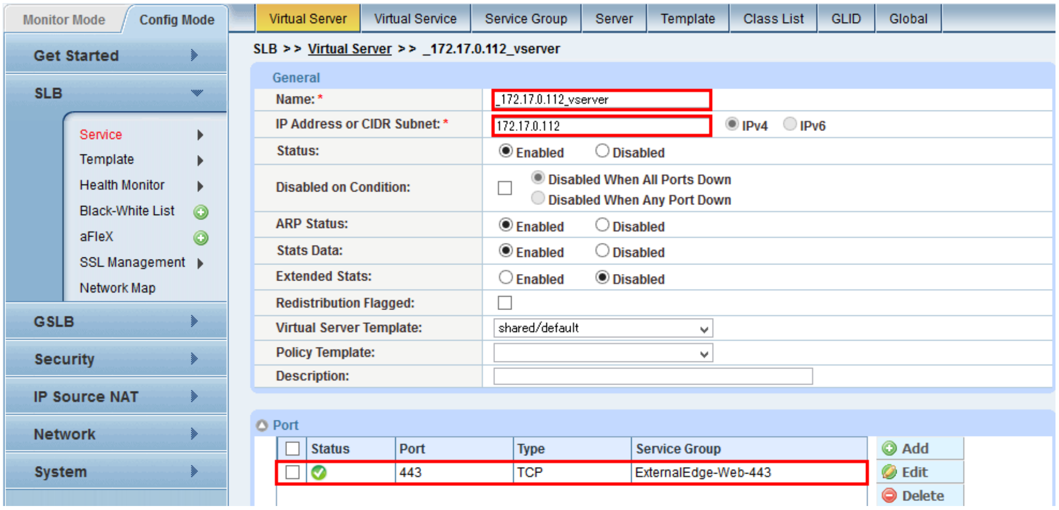
General

Name: *	_172.17.0.111_vserver
IP Address or CIDR Subnet: *	172.17.0.111 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
Virtual Server Template:	shared/default
Policy Template:	
Description:	

Port

□	Status	Port	Type	Service Group
□	✓	443	TCP	ExternalEdge-access-443

Figure 28: Virtual Server configuration for external Lync Access Edge Server



SLB >> Virtual Server >> _172.17.0.112_vserver

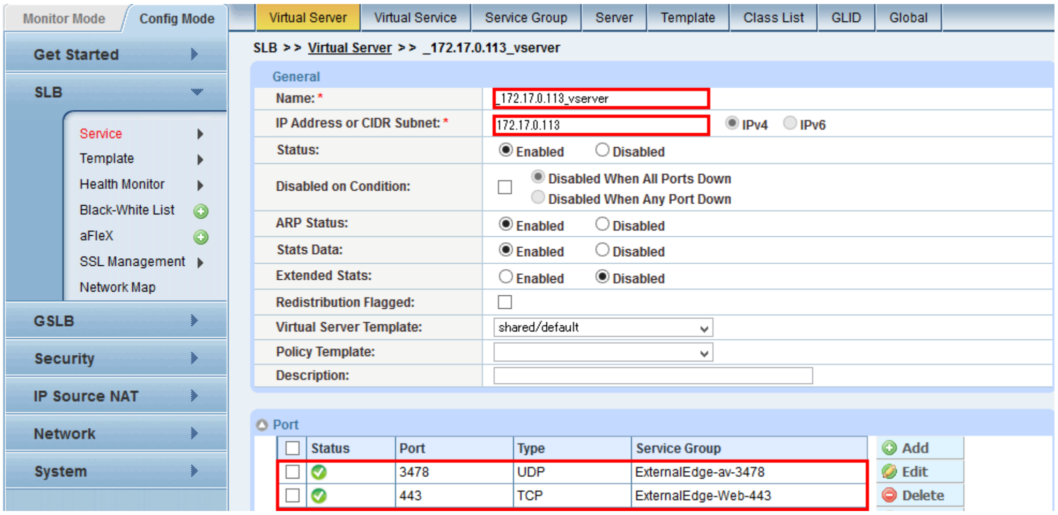
General

Name: *	_172.17.0.112_vserver
IP Address or CIDR Subnet: *	172.17.0.112 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
Virtual Server Template:	shared/default
Policy Template:	
Description:	

Port

□	Status	Port	Type	Service Group
□	✓	443	TCP	ExternalEdge-Web-443

Figure 29: Virtual Server configuration for external Lync Web Conf Edge Server



SLB >> Virtual Server >> _172.17.0.113_vserver

General

Name: *	_172.17.0.113_vserver
IP Address or CIDR Subnet: *	172.17.0.113 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
Virtual Server Template:	shared/default
Policy Template:	
Description:	

Port

□	Status	Port	Type	Service Group
□	✓	3478	UDP	ExternalEdge-av-3478
□	✓	443	TCP	ExternalEdge-Web-443

Figure 30: Virtual Server configuration for external Lync A/V Edge Server

6 Internal Edge Load Balancing

If a load balancer is deployed for an external Lync Edge pool, it is required that an internal Lync Edge pool be deployed with load balancer as well. If DNS load balancing is used for an external Lync Edge pool, it should be used for the internal Lync Edge pool as well. The internal Lync Edge pool handles traffic from internal Lync server components or from Lync clients to remote Lync clients. An internal Lync Edge pool doesn't have multiple roles, unlike an external Lync Edge pool (Access, Web Conf, A/V).

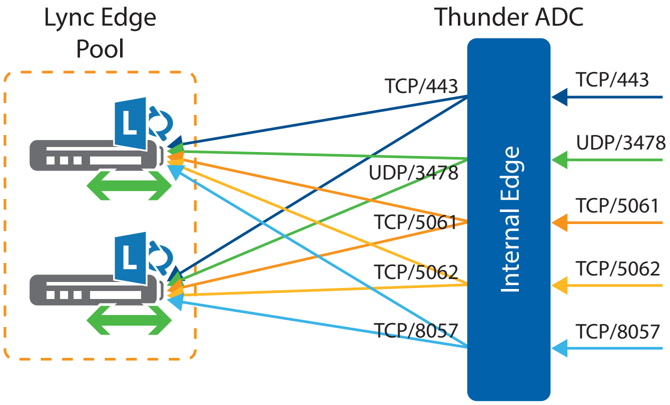


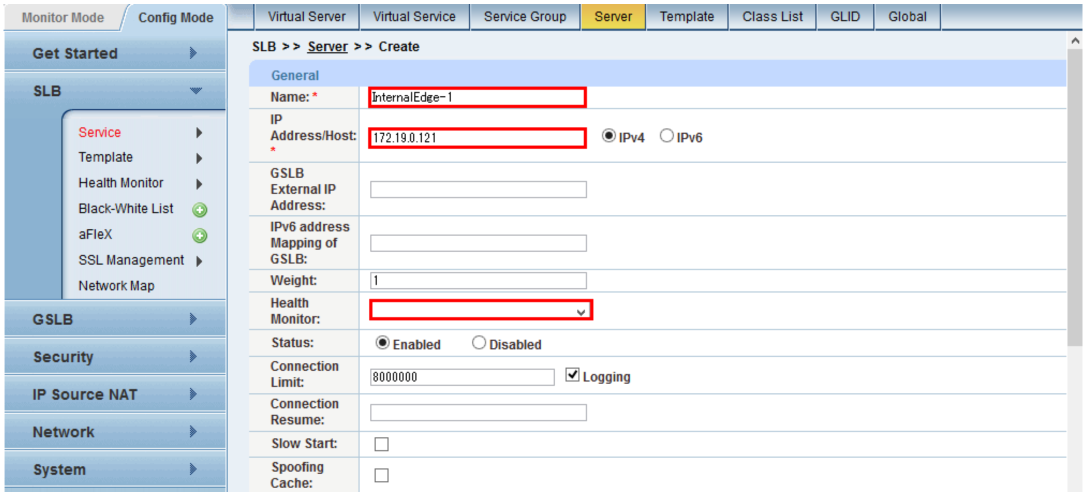
Figure 31: Load balancing image diagram for Internal Lync Edge pool

This section describes how to configure an internal Lync Edge pool (services) on the Thunder ADC.

6.1 Server Configuration

Create an internal Lync Edge server on the Thunder ADC.

1. Move to Config Mode > SLB > Service > Server.
2. Click Add and add an Internal Edge server as below.
3. The following input is used in this test environment:
   a. Name: InternalEdge-1
   b. IP Address/Host: 172.19.0.121
   c. Health Monitor: leave blank (The Health Monitor is configured in a Service group)



SLB >> Server >> Create

General

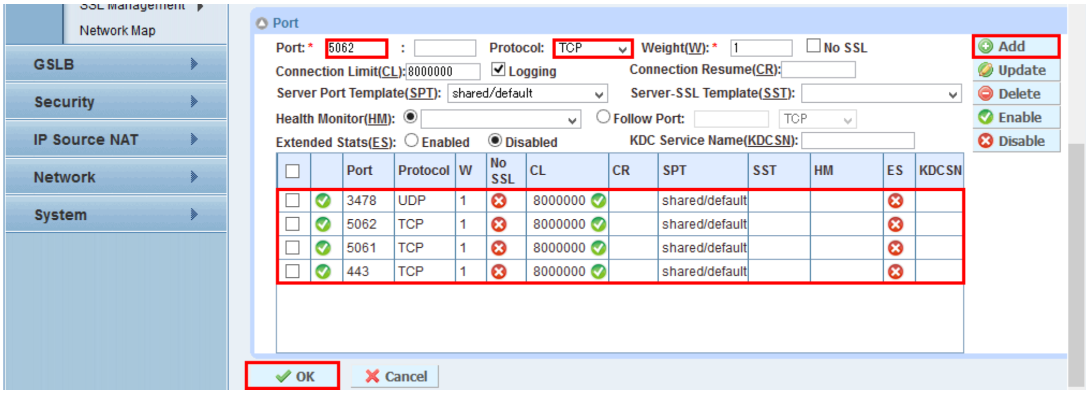
Name: *	InternalEdge-1
IP Address/Host: *	172.19.0.121 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□

Figure 32: Internal Lync Edge Server configuration

4. Scroll down to the Port section and add port information.

   a. Add a port number, select a proper protocol type, choose blank in Health Monitor (HM), and click Add.

   b. Repeat the above step for all required ports. Please refer to Table 3 to clarify which ports should be configured.



Port:* 5062 : Protocol: TCP Weight(W):* 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): shared/default Server-SSL Template(SST):

Health Monitor(HM): ● Follow Port: TCP

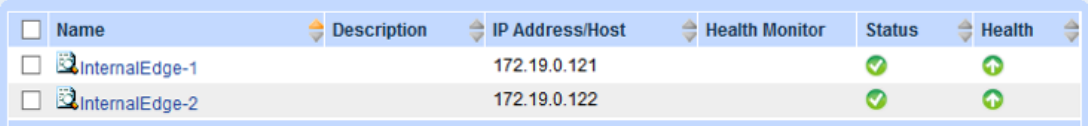
Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	3478	UDP	1	✗	8000000 ✓		shared/default			✗	
□	✓	5062	TCP	1	✗	8000000 ✓		shared/default			✗	
□	✓	5061	TCP	1	✗	8000000 ✓		shared/default			✗	
□	✓	443	TCP	1	✗	8000000 ✓		shared/default			✗	

Figure 33: Internal Lync Edge Server port configuration

5. Click OK after the configuration is completed and click Save to save the configuration.

6. Repeat the above steps until all internal Lync Edge server configurations are completed. In this test environment, A10LY13EGS2 is configured additionally.



□	Name	Description	IP Address/Host	Health Monitor	Status	Health
□	InternalEdge-1		172.19.0.121		✓	↑
□	InternalEdge-2		172.19.0.122		✓	↑

Figure 34: Internal Lync Edge Server list

6.2 Service Group Configuration

Next, create a service group for Internal Lync Edge servers on the Thunder ADC.

1. Move to Config Mode > SLB > Service > Service Group.

2. Click Add and create a new service group for an internal Lync Edge pool.

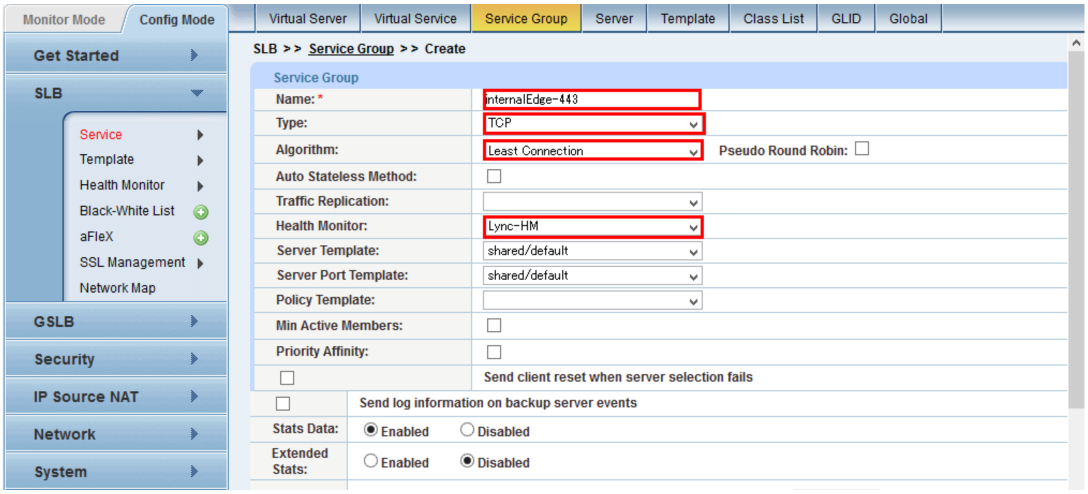
3. In this test environment the following input is used:

   a. Name: internalEdge-443

   b. Type: TCP

   c. Algorithm: Least Connection

   d. Health Check: Lync-HM



SLB >> Service Group >> Create

Service Group

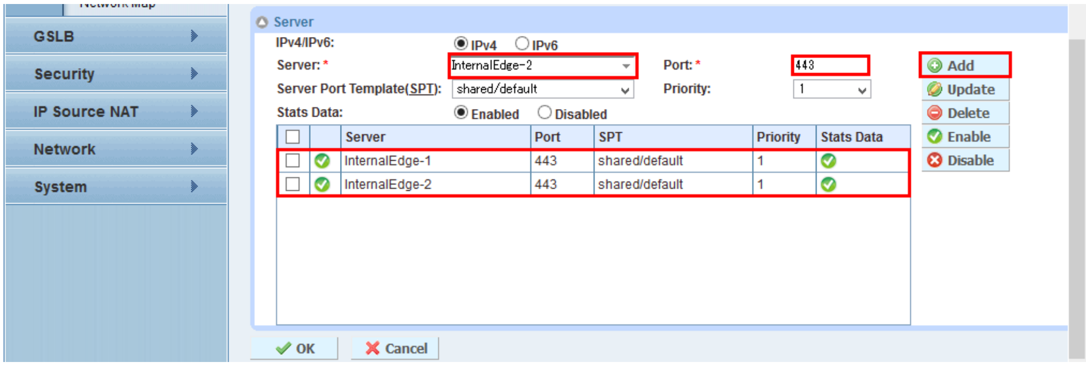
Name:*	internalEdge-443
Type:	TCP
Algorithm:	Least Connection Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	Lync-HM
Server Template:	shared/default
Server Port Template:	shared/default
Policy Template:	
Min Active Members:	□
Priority Affinity:	□
□	Send client reset when server selection fails
□	Send log information on backup server events
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled

Figure 35: Internal Lync Edge service group configuration

Note: The set of real server, port and server selection algorithm are defined in a service group. Multiple service groups need to be defined if an application uses multiple ports on a single IP.

e. Scroll down to the Server section and add more servers with an appropriate port.

f. Click **OK** after the configuration is done and click Office to save the configuration.



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server:* InternalEdge-2   Port:* 443

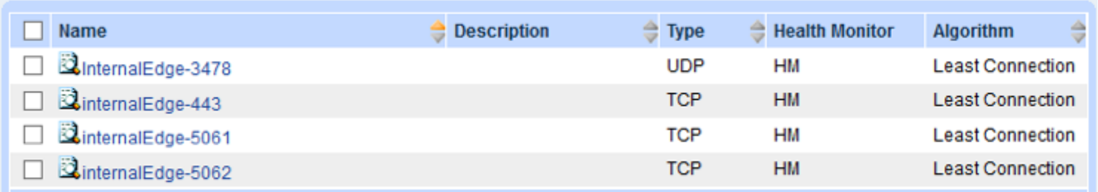
Server Port Template(SPT): shared/default   Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	InternalEdge-1	443	shared/default	1	✓
□	✓	InternalEdge-2	443	shared/default	1	✓

Figure 36: Internal Lync Edge service group – server list

g. Repeat the above steps (from Step a to Step f) for all required service groups with an appropriate port. Please refer to Table 3 to clarify which service groups should be configured.



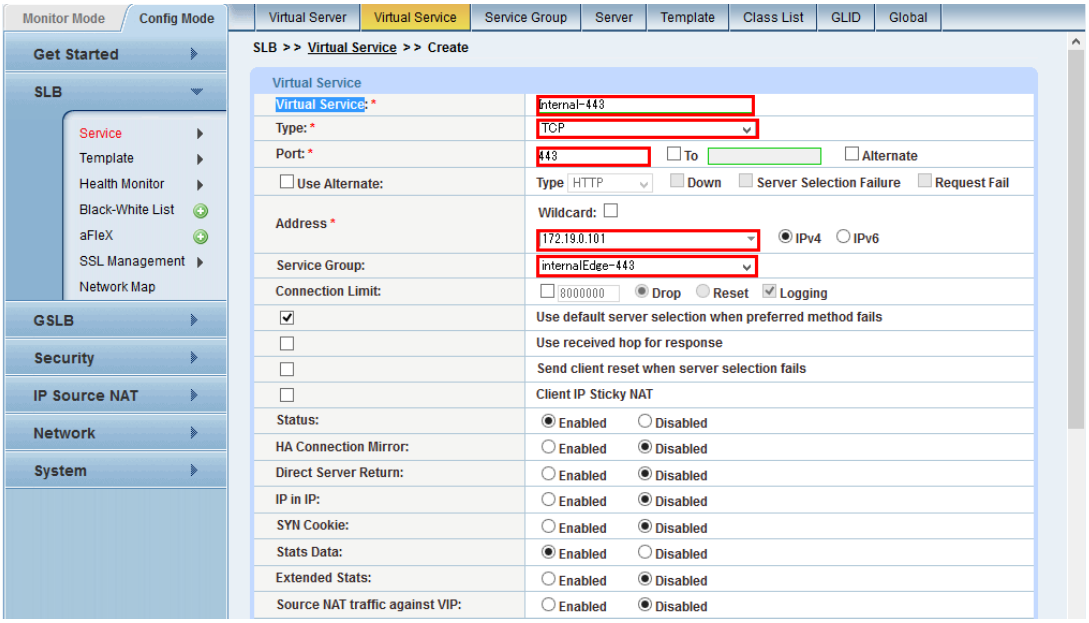
□	Name	Description	Type	Health Monitor	Algorithm
□	InternalEdge-3478		UDP	HM	Least Connection
□	internalEdge-443		TCP	HM	Least Connection
□	internalEdge-5061		TCP	HM	Least Connection
□	internalEdge-5062		TCP	HM	Least Connection

Figure 37: Internal Lync Edge service group list

6.3 Virtual Service Configuration

Configure virtual servers for an internal Lync Edge pool at the virtual service configuration level, as well as for an external Lync Edge pool configuration.

1. Move to **Config Mode** > **SLB** > **Service** > **Virtual Service**.
2. Click **Add** and create a new virtual service.
3. In this test environment the following input is used:
   a. Virtual Service: **Internal-443**
   b. Type: **TCP**
   c. Port: **443**
   d. Address: **172.19.0.101**
   e. Service Group: **InternalEdge-443**



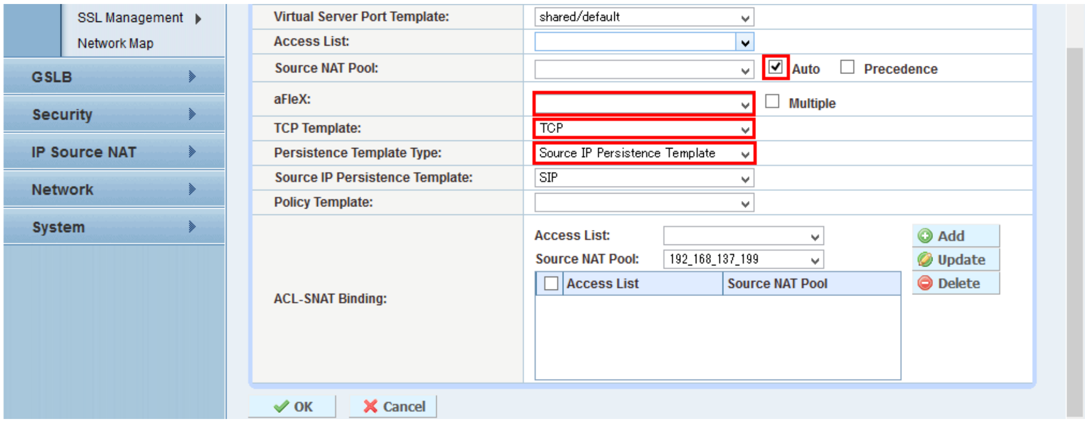
SLB >> Virtual Service >> Create

Virtual Service

Virtual Service: *	Internal-443
Type: *	TCP
Port: *	443 □ To □ Alternate
□ Use Alternate:	Type HTTP □ Down □ Server Selection Failure □ Request Fail
Address *	Wildcard: □ 172.19.0.101 ● IPv4 ○ IPv6
Service Group:	internalEdge-443
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
HA Connection Mirror:	○ Enabled ● Disabled
Direct Server Return:	○ Enabled ● Disabled
IP in IP:	○ Enabled ● Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 38: Virtual service configuration for an internal Lync Edge pool

4. Set the following data as a feature template:
   a. Source NAT Pool: **Auto**
   b. TCP Template: **TCP**
   c. Persistence Template Type: **Source IP Persistence**
   d. Source IP Persistence Template: **SIP**

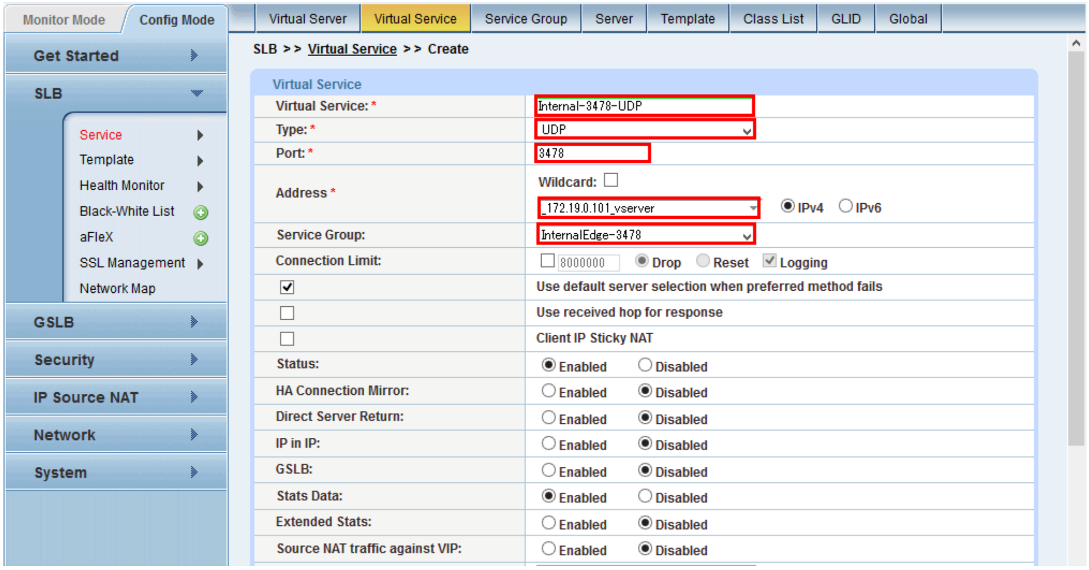


Virtual Server Port Template:	shared/default
Access List:	
Source NAT Pool:	☑ Auto □ Precedence
aFleX:	□ Multiple
TCP Template:	TCP
Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	SIP
Policy Template:	
ACL-SNAT Binding:	Access List: Source NAT Pool: 192_168_137_199 □ Access List | Source NAT Pool

Figure 39: Virtual service feature template for internal Lync Edge pool

Note: Please refer to Table 3 to clarify what feature template and persistence should be configured.

5. Click **OK** after the configuration is completed and click **Save** to save the configuration.
6. Repeat the above steps (from 1 to 3) for the remaining services (UDP/3478, TCP/5061, TCP/5062). Feature templates are common except UDP/3478.
7. The following input is used for a virtual service with UDP/3478:
   a. Virtual Service: **Internal-3478-UDP**
   b. Type: **UDP**
   c. Port: **3478**
   d. Address: **_172.19.0.101_vserver** (Already defined in the previous step)
   e. Service Group: **InternalEdge-3478**
   f. Source NAT Pool: **Auto**
   g. Source IP Persistence: **SIP**

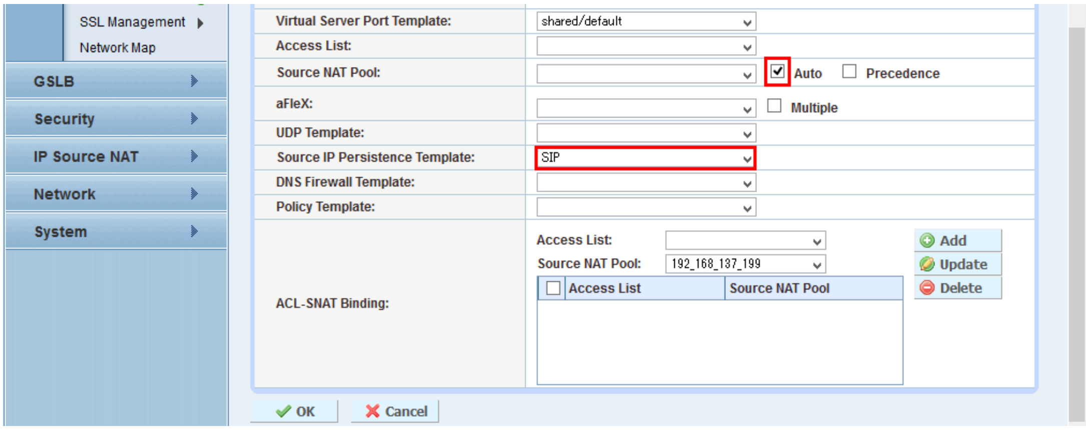


SLB >> Virtual Service >> Create

Virtual Service

Virtual Service: *	Internal-3478-UDP
Type: *	UDP
Port: *	3478
Address *	Wildcard: □ _172.19.0.101_vserver ● IPv4 ○ IPv6
Service Group:	InternalEdge-3478
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
HA Connection Mirror:	○ Enabled ● Disabled
Direct Server Return:	○ Enabled ● Disabled
IP in IP:	○ Enabled ● Disabled
GSLB:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 40: Virtual service configuration for internal Lync Edge pool UDP/3478

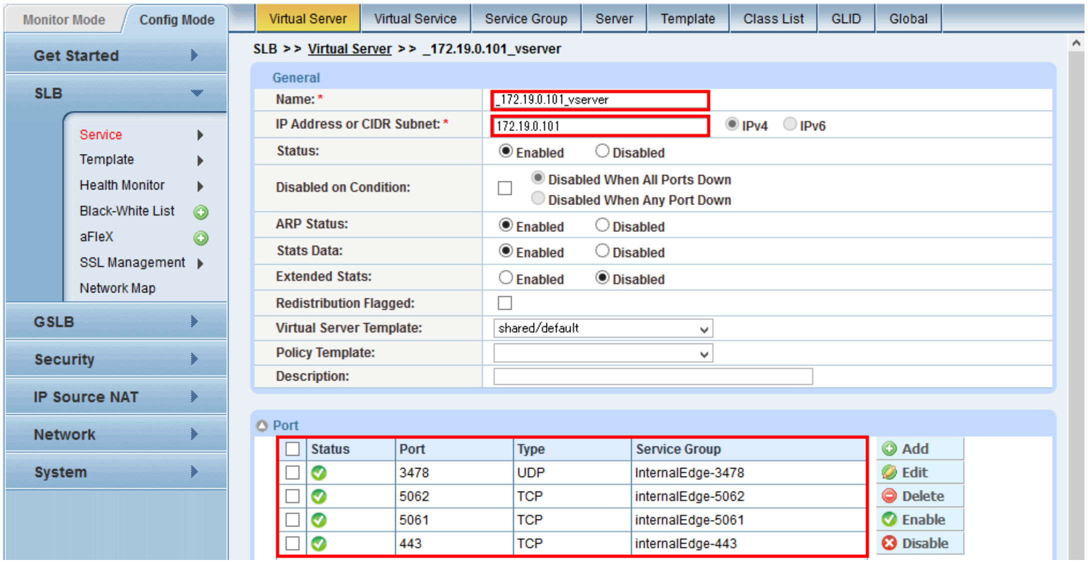


Virtual Server Port Template:	shared/default
Access List:	
Source NAT Pool:	☑ Auto ☐ Precedence
aFleX:	☐ Multiple
UDP Template:	
Source IP Persistence Template:	SIP
DNS Firewall Template:	
Policy Template:	
ACL-SNAT Binding:	Access List: Source NAT Pool: 192_168_137_199

☐ Access List	Source NAT Pool

Figure 41: Virtual service feature template for internal Lync Edge pool UDP/3478

Note*: Please refer to Table 3 to clarify what feature template and persistence should be configured.*



SLB >> Virtual Server >> _172.19.0.101_vserver

General

Name: *	_172.19.0.101_vserver
IP Address or CIDR Subnet: *	172.19.0.101 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	☐ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	☐
Virtual Server Template:	shared/default
Policy Template:	
Description:	

Port

☐	Status	Port	Type	Service Group
☐	✓	3478	UDP	InternalEdge-3478
☐	✓	5062	TCP	internalEdge-5062
☐	✓	5061	TCP	internalEdge-5061
☐	✓	443	TCP	internalEdge-443

Figure 42: Virtual server configuration for Internal Lync Edge pool

Note*: Please refer to Table 3 to clarify which ports should be defined for internal Lync Edge pool.*

7 Load Balancing for Office Web Apps Farm

This section describes how to configure load balancing for Office Web Apps farm on the Thunder ADC. SSL offload configuration is recommended for Office Web Apps server according to the Microsoft Tech Net site. Additionally, other server offload templates (compression, RAM caching, connection reuse and etc.) on the Thunder ADC would be effective for it.

An image diagram illustrating load balancing for Office Web Apps is shown in Figure 8.

7.1 Server Configuration

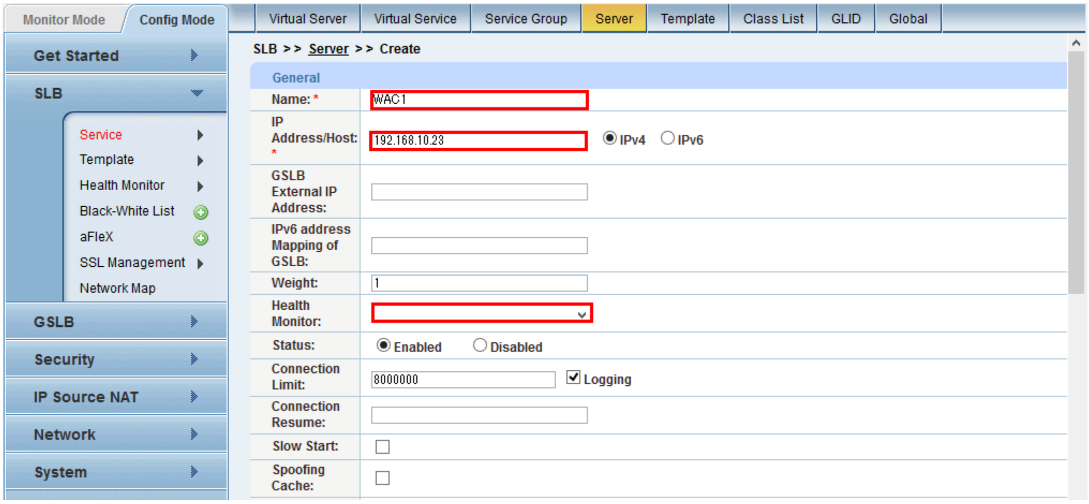
Add an Office Web Apps server on the Thunder ADC.

1. Move to **Config Mode** > **SLB** > **Service** > **Server.**
2. Click **Add** and create a new Office Web Apps Server.
3. In this test environment the following input is used:

    a. Name: **WAC1**

    b. IP Address/Host: **192.168.10.23**

    c. Health Monitor: leave blank (Health Monitor is configured in a Service group)



SLB >> Server >> Create

General

Name: * WAC1

IP Address/Host: * 192.168.10.23 ● IPv4 ○ IPv6

GSLB External IP Address:

IPv6 address Mapping of GSLB:

Weight: 1

Health Monitor:

Status: ● Enabled ○ Disabled

Connection Limit: 8000000 ☑ Logging

Connection Resume:

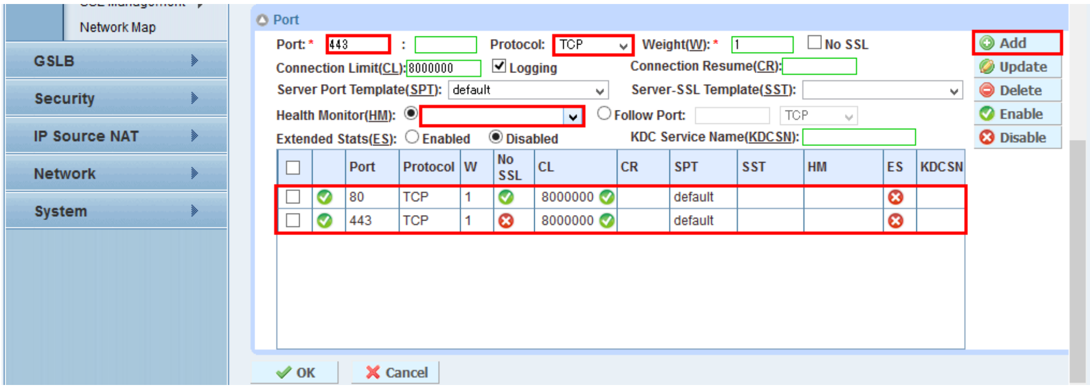
Slow Start: □

Spoofing Cache: □

Figure 43: Office Web Apps server configuration

4. Scroll down to the **Port** setting section and add port information.

    a. In this environment, port number 80 is added with "No SSL" checked and port number 443 is added without "No SSL" checked. Choose blank in Health Monitor (HM) and click **Add**.



Port:* 443 : Protocol: TCP Weight(W):* 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Server-SSL Template(SST):

Health Monitor(HM): ● ○ Follow Port: TCP

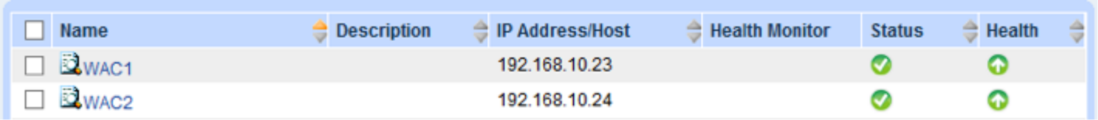
Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	80	TCP	1	✓	8000000 ✓		default			✗	
□	✓	443	TCP	1	✗	8000000 ✓		default			✗	

Figure 44: Office Web Apps server port configuration

Note: *The port TCP/443 configuration is not required if SSL offload is enabled. However in this test environment both TCP/80 and TCP/443 are configured.*

5. Click **OK** after the configuration is completed and click **Save** to save the configuration.
6. Repeat the above steps until all Office Web Apps configurations are completed. In this test environment, A10LY13WAC2 is configured as WAC2 additionally.



□	Name	Description	IP Address/Host	Health Monitor	Status	Health
□	WAC1		192.168.10.23		✓	⬆
□	WAC2		192.168.10.24		✓	⬆

Figure 45: Office Web Apps server list

7.2 Service Group Configuration

Next, configure a service group for Office Web Apps farm on the Thunder ADC.

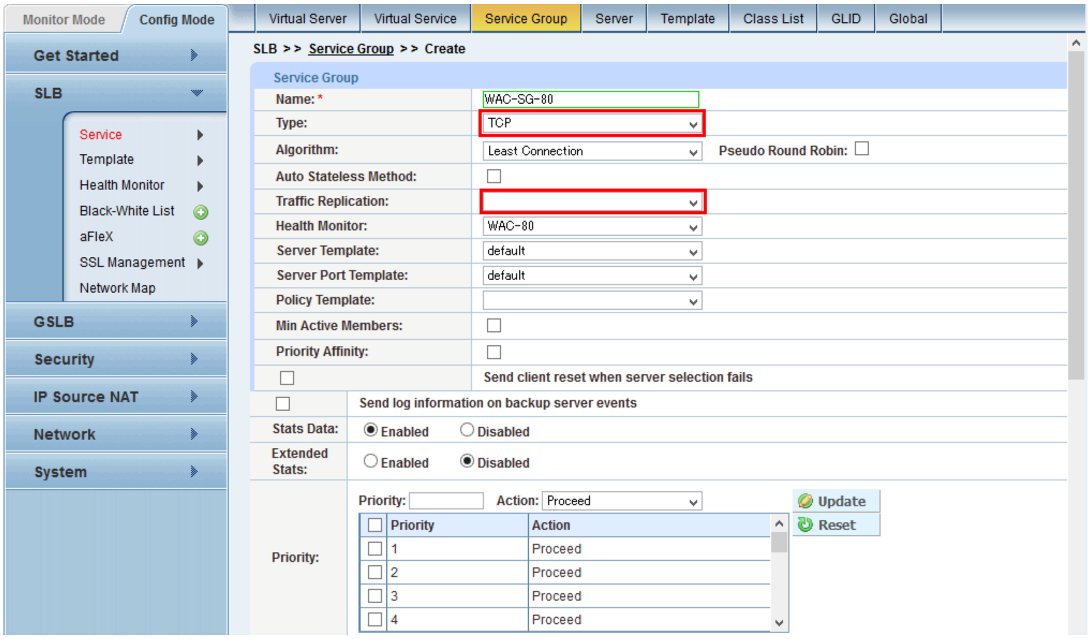
1. Move to **Config Mode** > **SLB** > **Service** > **Service Group**.
2. Click Add to create a new service group.
3. In this test environment the following input is used:

   a. Name: **WAC-SG-80**

   b. Type: **TCP**

   c. Algorithm: **Least Connection**

   d. Health Monitor: **WAC-80** (Detail is provided in Section 7.4)



SLB >> Service Group >> Create

Service Group

Name: *	WAC-SG-80
Type:	TCP
Algorithm:	Least Connection — Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	WAC-80
Server Template:	default
Server Port Template:	default
Policy Template:	
Min Active Members:	□
Priority Affinity:	□
□	Send client reset when server selection fails
□	Send log information on backup server events
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled

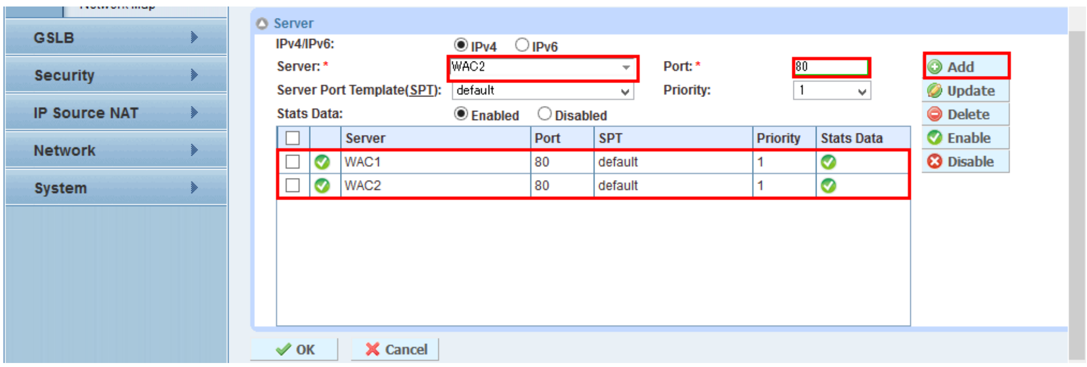
Priority: Priority: ___ Action: Proceed

□	Priority	Action
□	1	Proceed
□	2	Proceed
□	3	Proceed
□	4	Proceed

Figure 46: Service group configuration for Office Web Apps farm

Note: The set of real server, port and server selection algorithm are defined in a service group. Multiple service groups are needed if multiple ports are used on single IP.

e. Scroll down to the **Server** setting section and add more servers with an appropriate port. In this test environment, WAC1 and WAC2 are added with port number 80.



Server

IPv4/IPv6: ● IPv4 ○ IPv6
Server: * WAC2 Port: * 80
Server Port Template(SPT): default Priority: 1
Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	WAC1	80	default	1	✓
□	✓	WAC2	80	default	1	✓

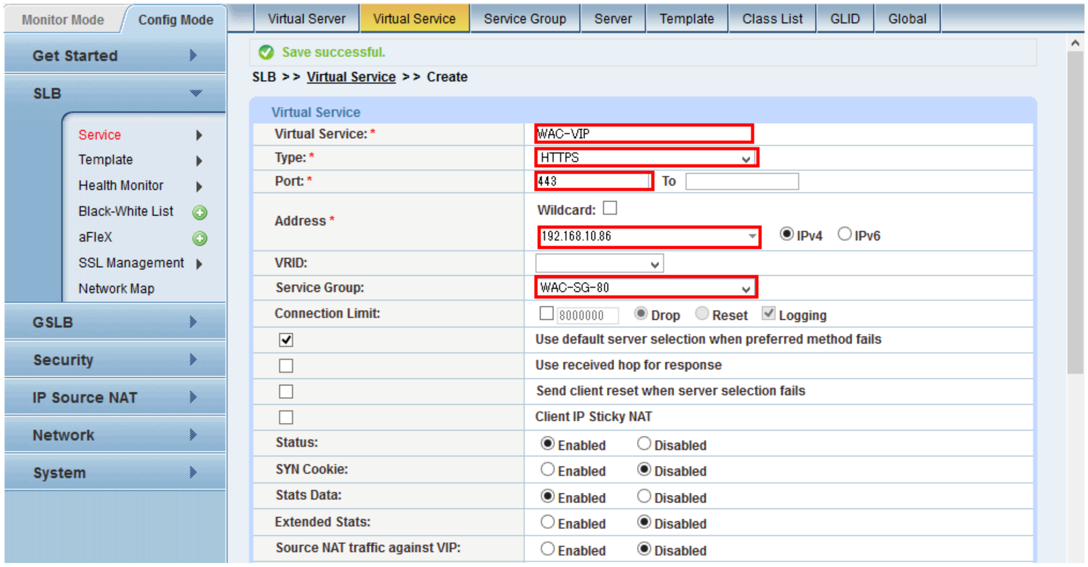
Figure 47: Server list in Office Web Apps farm service group

4. Click **OK** after the configuration is completed and click **Save** to save the configuration.

7.3 Virtual Service Configuration

Configure a virtual server for Office Web Apps farm at the virtual service configuration level as well as an external Lync Edge pool configuration.

1. Move to **Config Mode** > **SLB** > **Service** > **Virtual Service**.
2. Click **Add** to create a new virtual service for Office Web Apps farm.
3. The following input is configured in this test environment:
   a. Virtual Service: **WAC-VIP**
   b. Type: **https**
   c. Port: **443**
   d. Address: **192.168.10.86**
   e. Service Group: **WAC-SG-80**



Save successful.

SLB >> Virtual Service >> Create

Virtual Service

Virtual Service: *	WAC-VIP
Type: *	HTTPS
Port: *	443 To
Address *	Wildcard: □ 192.168.10.86 ● IPv4 ○ IPv6
VRID:	
Service Group:	WAC-SG-80
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 48: Virtual Service configuration for Office Web Apps farm

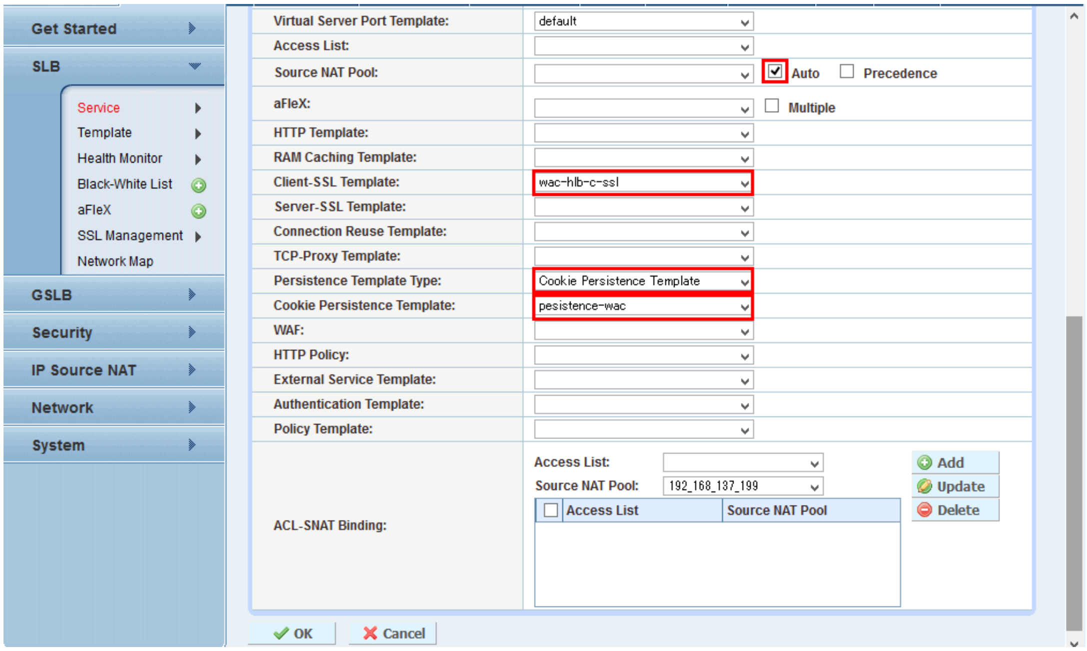
Set the following info as a feature template:

f. Source NAT Pool: **Auto**

g. Client SSL Template: **wac-hlb-c-ssl** (Detail is provided in Section 7.5)

h. Persistence Template Type: **Cookie Persistence Template**

i. Cookie Persistence Template: **persistence-wac** (Detail is provided in Section 7.6)



Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	☑ Auto □ Precedence
aFleX:	□ Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	wac-hlb-c-ssl
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	Cookie Persistence Template
Cookie Persistence Template:	pesistence-wac
WAF:	
HTTP Policy:	
External Service Template:	
Authentication Template:	
Policy Template:	
ACL-SNAT Binding:	Access List: Source NAT Pool: 192_168_137_199 □ Access List | Source NAT Pool

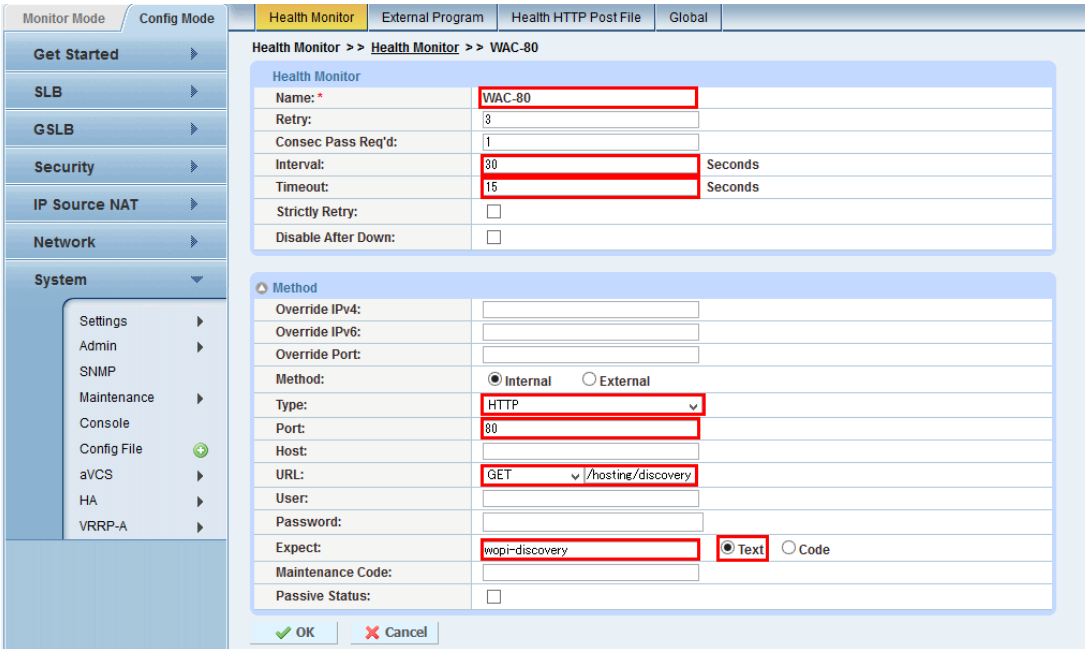
Figure 49: Feature template configuration for Office Web Apps farm virtual service

4. Click **OK** after the configuration is completed and click **Save** to save the configuration.

7.4 Health Monitor Configuration

This section describes how to configure a Health Monitor for an Office Web Apps farm service group. The Office Web Apps server returns "wopi-discovery" if a proper GET request comes to the "/hosting/discovery" URI on Office Web Apps Server. Utilize this process as a Health Monitor.

1. Move to Config Mode > SLB > Health Monitor > Health Monitor.
2. Click Add to create a new Health Monitor for Office Web Apps
3. In this test environment the following input is used:
   a. Name: WAC-80
   b. Interval: 30
   c. Timeout: 10
   d. Type: HTTP
   e. Port: 80
   f. URL: GET /hosting/discovery
   g. Expect: wopi-discovery (text)



Health Monitor >> Health Monitor >> WAC-80

Health Monitor

Name: *	WAC-80	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	30	Seconds
Timeout:	15	Seconds
Strictly Retry:	□	
Disable After Down:	□	

Method

Override IPv4:		
Override IPv6:		
Override Port:		
Method:	● Internal ○ External	
Type:	HTTP	
Port:	80	
Host:		
URL:	GET /hosting/discovery	
User:		
Password:		
Expect:	wopi-discovery	● Text ○ Code
Maintenance Code:		
Passive Status:	□	

Figure 50: Health Monitor configuration for Office Web Apps

Note: Both the Interval and Timeout value depend on the service level in the actual environment. Please ask the IT management department if needed.

4. Click OK after the configuration is completed and click Save to save the configuration.

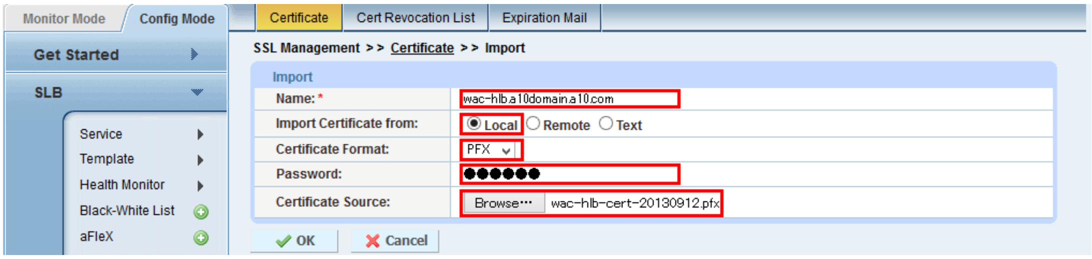
7.5 Client SSL Template Configuration

This section describes how to configure a client template for SSL offload for Office Web Apps (WAC) farm.

First, import the certificate for Office Web Apps farm. Usually it is issued by an internal enterprise CA.

1. Move to Config Mode > SLB > SSL Management > Certificate.
2. Click Import

3. In this test environment the following input is used:
   a. Name: **wac-hlb.a10domain.a10.com**
   b. Import Certificate From : **Local**
   c. Certificate Format: **PFX**
   d. Password: **Actual password for secret key** filed with certificate.
   e. Certificate Source: **Actual SSL Server Certificate filename** for Office Web Apps farm.



SSL Management >> Certificate >> Import

Import

Name:*	wac-hlb.a10domain.a10.com
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	PFX
Password:	●●●●●●
Certificate Source:	Browse… wac-hlb-cert-20130912.pfx

Figure 51: Import Office Web Apps SSL Server certificate

Note*: In this test environment, the SSL server certificate issued by an internal Windows server CA is used. An SSL server certificate issued by a public CA (like VeriSign or DigiCert) can be used as well.*

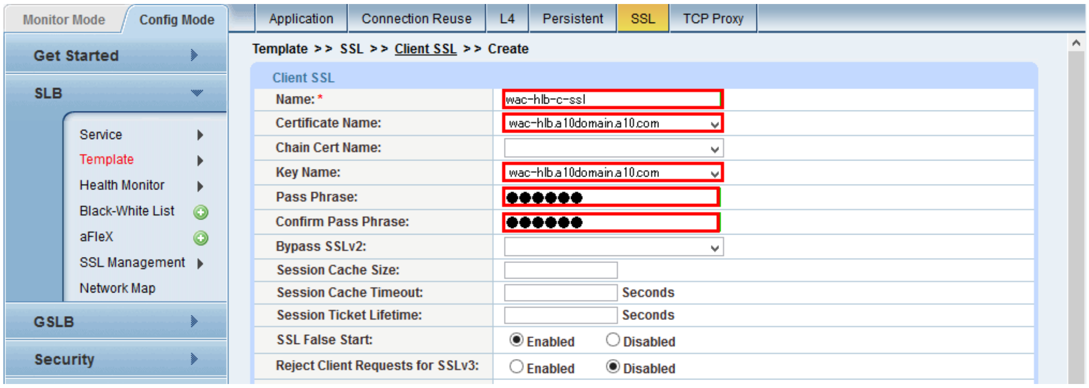
4. Click **OK** after the import is completed and click **Save** to save the configuration.

Next, create a Client SSL template after the certificate is imported.

1. Move to **Config Mode** > **SLB** > **Template** > **SSL** > **Client SSL.**
2. Click **Add** and create a new client SSL template. In this test environment, the following input is used:
   a. Name: **wac-hlb-c-ssl**
   b. Certificate Name: **wac-hlb.a10domain.a10.com**
   c. Key Name: **wac-hlb.a10domain.a10.com**

Note*: The Key Name is different from the Certificate Name if the secret key isn't stored within the certificate file.*

   d. Password: Password for secret key



Template >> SSL >> Client SSL >> Create

Client SSL

Name:*	wac-hlb-c-ssl
Certificate Name:	wac-hlb.a10domain.a10.com
Chain Cert Name:	
Key Name:	wac-hlb.a10domain.a10.com
Pass Phrase:	●●●●●●
Confirm Pass Phrase:	●●●●●●
Bypass SSLv2:	
Session Cache Size:	
Session Cache Timeout:	Seconds
Session Ticket Lifetime:	Seconds
SSL False Start:	● Enabled ○ Disabled
Reject Client Requests for SSLv3:	○ Enabled ● Disabled

Figure 52: Client SSL template configuration for Office Web Apps

3. Click **OK** after the configuration is completed and click **Save** to save the configuration.

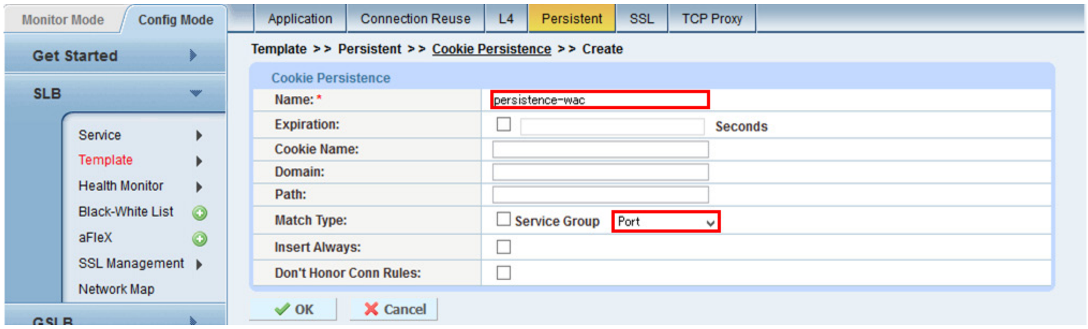
7.6 Cookie Persistence Configuration

This section describes how to configure Cookie Persistence, which is used for Office Web Apps farm.

1. Move to Config Mode > SLB > Template > Cookie Persistence.
2. Click Add and create a new Cookie Persistence Template using the following procedure in this test environment:

   a. Name: persistence-wac

   b. Match Type: Port (Default value)



Template >> Persistent >> Cookie Persistence >> Create

Cookie Persistence

Name: *	persistence-wac
Expiration:	□ Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	□ Service Group Port
Insert Always:	□
Don't Honor Conn Rules:	□

Figure 53: Cookie Persistence Template for Office Web Apps farm

3. Click OK after the configuration is completed and click Save to save the configuration.

8 Reverse Proxy

This section describes how to configure Reverse Proxy for Lync Sever 2013 and Office Web Apps. Reverse Proxy is used for publishing Web Services of Lync Front End Server and Office Web Apps Server to remote access users through the Internet.

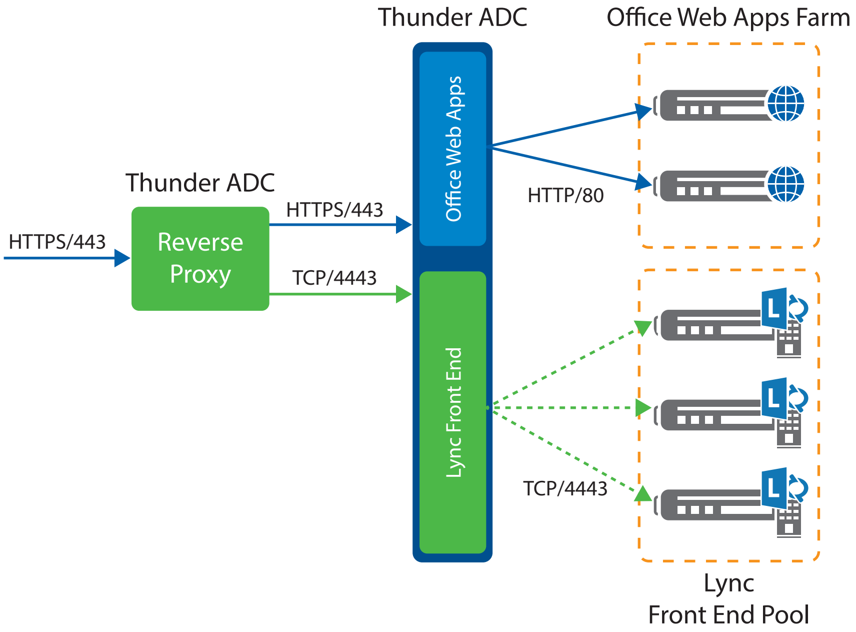


Figure 54: Load balancing image diagram for Reverse Proxy

8.1 Importing Certificate

First, import the SSL server certificate used for access from remote users. Usually it is issued by a public CA (not an internal enterprise CA).

Also, import the root certificate of the CA which issues the internal SSL server certificate for Lync Front End Pool and Office Web Apps Farm. Usually the internal enterprise CA is used for issuing internal SSL server certificate.

1. Move to **Config Mode** > **SLB** > **SSL Management** > **Certificate.**
2. Click **Add** and import the SSL server certificate for remote user access with the following procedure. In this test environment, the certificate file contains published FQDN of both Lync Server 2013 Front End Pool and Office Web Apps Farm.

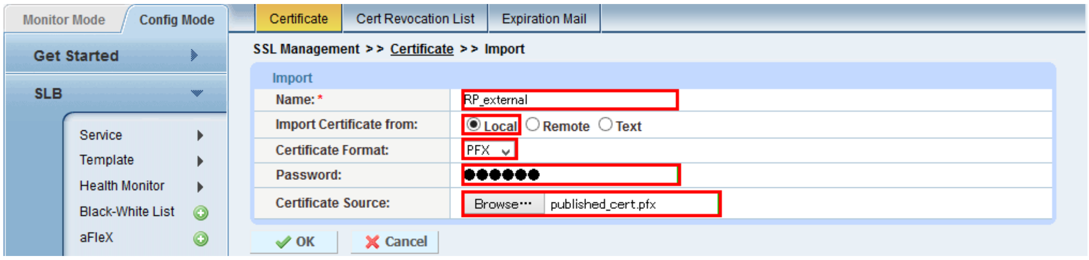
   a. Name: **RP_external**

   b. Import Certificate From: **Local**

   c. Certificate Format: **PFX**

   d. Password: **Password for secret key** stored within imported certificate file.

   e. Certificate Source: **Actual SSL Server Certificate filename**.



SSL Management >> Certificate >> Import

Import

Name: *	RP_external
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	PFX
Password:	●●●●●●
Certificate Source:	Browse… published_cert.pfx

Figure 55: Import SSL server certificate used for remote user access

3. Click **OK** after the import is completed and click **Save** to save the configuration.

Next, import the root certificate issued by an internal enterprise CA.

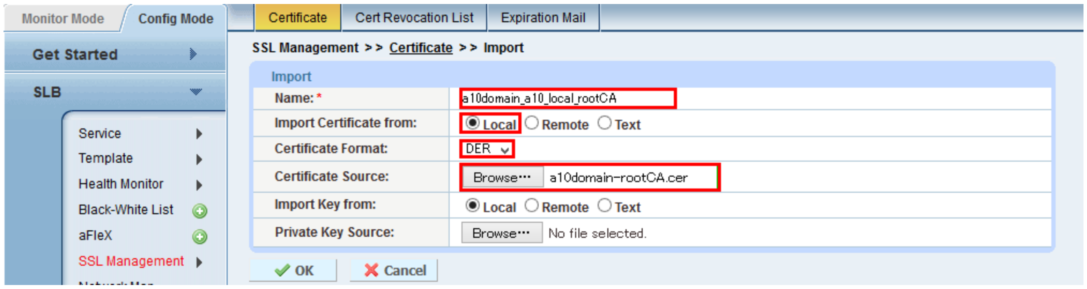
4. Click **Add** again and use the following procedure:

   a. Name: **a10domain_a10_local_rootCA**

   b. Import Certificate From: **Local**

   c. Certificate Format: **DER** (Choose proper Certificate File Format)

   d. Certificate Source: **Actual root certificate filename**



SSL Management >> Certificate >> Import

Import

Name: *	a10domain_a10_local_rootCA
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	DER
Certificate Source:	Browse… a10domain-rootCA.cer
Import Key from:	● Local ○ Remote ○ Text
Private Key Source:	Browse… No file selected.

Figure 56: Import the root certificate for access to Lync Server 2013 Front End pool and Office Web Apps Farm

5. Click **OK** after the import is completed and click **Save** to save the configuration.

8.2 SSL Template Configuration

Create a Client SSL template and a Server SSL template using the certificate imported in the previous section. The Server SSL template is required for establishing SSL sessions to the internal Lync Server 2013 Front End Server and Office Web Apps Server.

First, create a Client SSL template with the following procedure:

1. Move to **Config Mode** > **SLB** > **Template** > **SSL** > **Client SSL**.
2. Click **Add**. In this test environment, the following input is used:

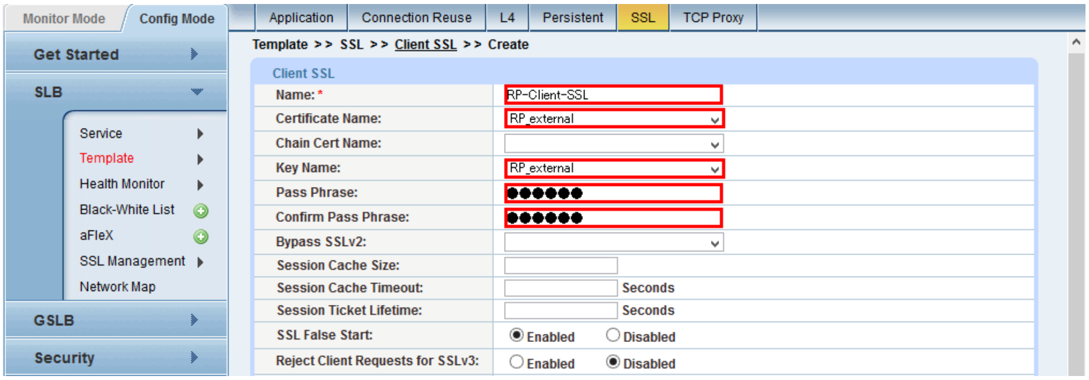
   a. Name: **RP-Client-SSL**

   b. Certificate Name: **RP-External**

   c. Key Name: **RP-External**

Note: The Key Name is different from the Certificate Name if the secret key isn't stored within the certificate file.

   d. Password: Password for secret key



Template >> SSL >> Client SSL >> Create

Client SSL

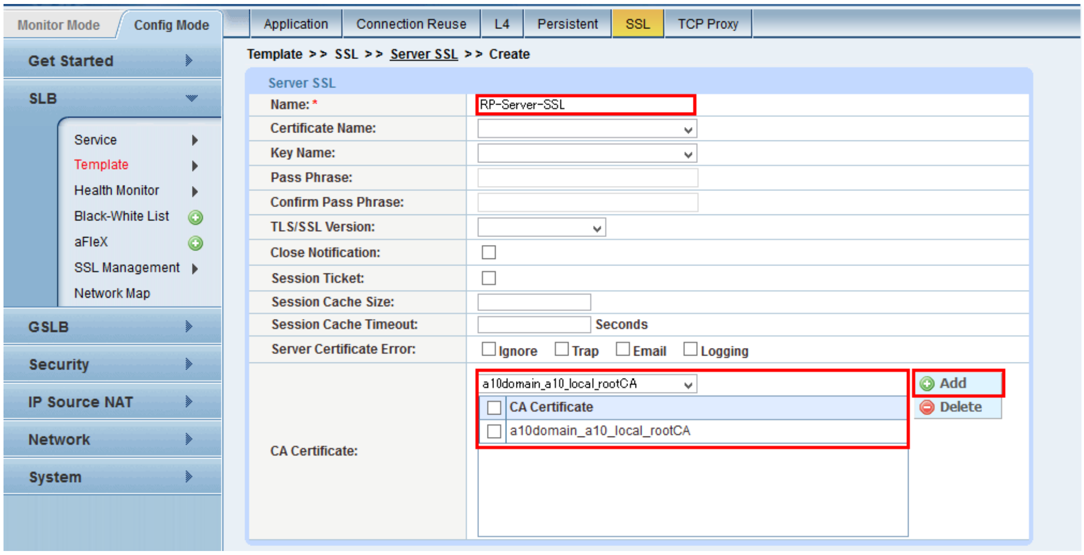
Name: *	RP-Client-SSL
Certificate Name:	RP_external
Chain Cert Name:	
Key Name:	RP_external
Pass Phrase:	●●●●●●
Confirm Pass Phrase:	●●●●●●
Bypass SSLv2:	
Session Cache Size:	
Session Cache Timeout:	Seconds
Session Ticket Lifetime:	Seconds
SSL False Start:	● Enabled ○ Disabled
Reject Client Requests for SSLv3:	○ Enabled ● Disabled

Figure 57: Client SSL template configuration for Reverse Proxy

3. Click **OK** after the configuration is completed and click **Save** to save the configuration.

Next create a Server SSL template with the following procedure:

4. Move to **Config Mode** > **SLB** > **Template** > **SSL** > **Server SSL**
5. Click **Add** and create a server SSL template. In this test environment, the following input is used:
   a. Name: **RP-Server-SSL**
   b. CA Certificate : Select **root certificate** for internal CA imported in previous section and click **Add**



Template >> SSL >> Server SSL >> Create

Server SSL

Name: *	RP-Server-SSL
Certificate Name:	
Key Name:	
Pass Phrase:	
Confirm Pass Phrase:	
TLS/SSL Version:	
Close Notification:	□
Session Ticket:	□
Session Cache Size:	
Session Cache Timeout:	Seconds
Server Certificate Error:	□ Ignore □ Trap □ Email □ Logging
CA Certificate:	a10domain_a10_local_rootCA □ CA Certificate □ a10domain_a10_local_rootCA

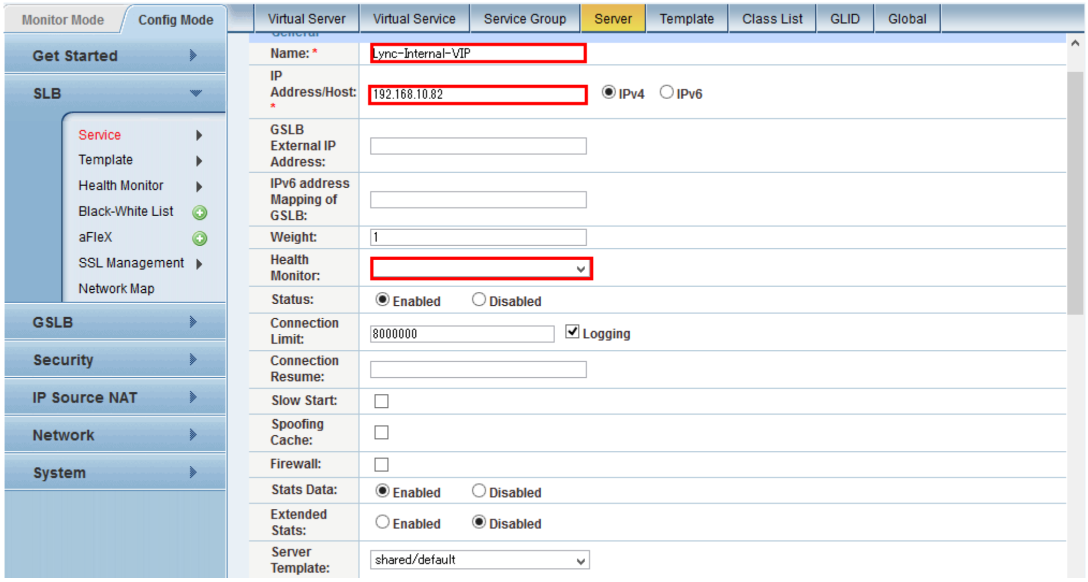
Figure 58: Server SSL template configuration for Reverse Proxy

6. Click **OK** after the configuration is completed and click **Save** to save the configuration.

8.3 Server Configuration

Configure the server that should be published to the Internet through Reverse Proxy.

1. Move to **Config Mode** > **SLB** > **Service** > **Server**.
2. Click **Add** and create a server using the VIP for Lync Server 2013 Front End Pool. It is already configured in Chapter 4 in this example configuration.
3. In this test environment, the following input is used for the server configuration:
   a. Name: **Lync-Internal-VIP**
   b. IP Address/Host: **192.168.10.82**
   c. Health Monitor: leave blank (The Health Monitor is configured in a Service group)



Name:* Lync-Internal-VIP

IP Address/Host:* 192.168.10.82 ● IPv4 ○ IPv6

GSLB External IP Address:

IPv6 address Mapping of GSLB:

Weight: 1

Health Monitor:

Status: ● Enabled ○ Disabled

Connection Limit: 8000000 ☑ Logging

Connection Resume:

Slow Start: □

Spoofing Cache: □

Firewall: □

Stats Data: ● Enabled ○ Disabled

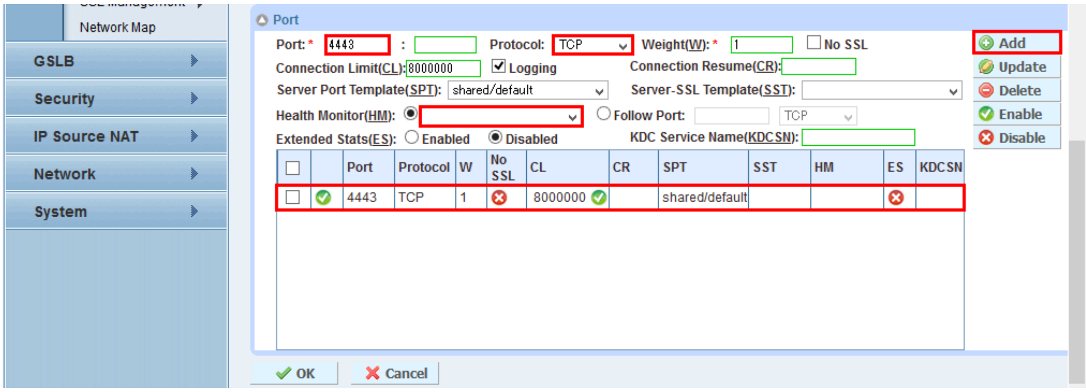
Extended Stats: ○ Enabled ● Disabled

Server Template: shared/default

Figure 59: Reverse Proxy server configuration for Lync Server 2013 Front End pool

4. Scroll down to the Port section and add port information.

   a. Enter TCP/4443, choose blank in Health Monitor (HM), and click **Add**.



Port:* 4443 : Protocol: TCP Weight(W):* 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): shared/default Server-SSL Template(SST):

Health Monitor(HM): ● ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	4443	TCP	1	✗	8000000 ✓		shared/default			✗	

Figure 60: Reverse Proxy server port configuration for Lync Server 2013 Front End pool

5. Click **OK** after the configuration is completed and click **Save** to save the configuration.

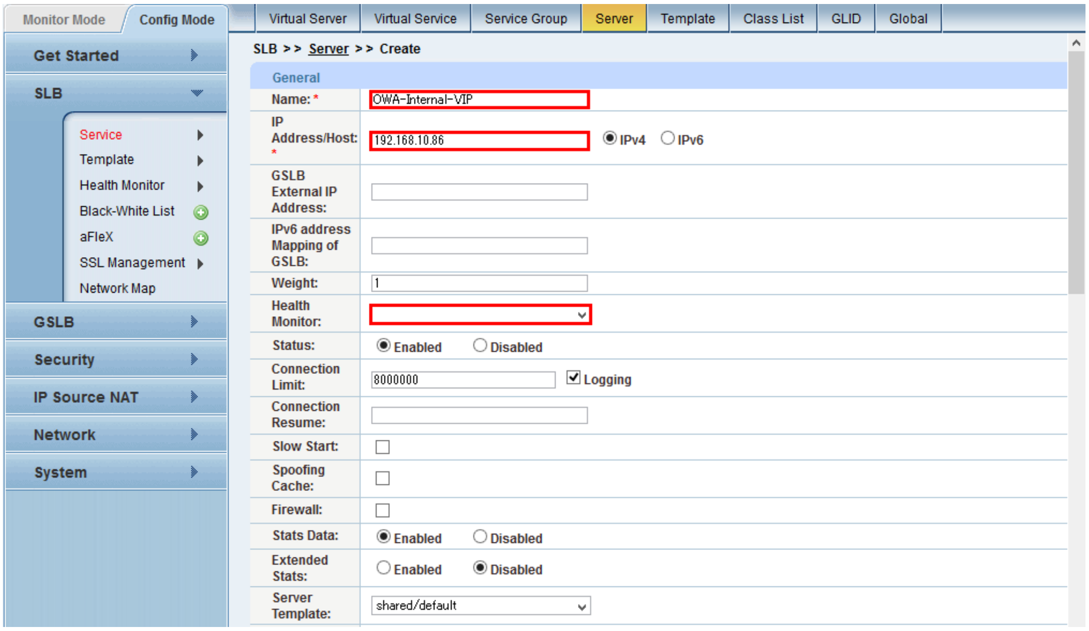
6. Click **Add** again and then create a new server using the VIP for Office Web Apps farm created in Section 7.3.

7. In this test environment, the following input is used:

   a. Name: **OWA-Internal-VIP**

   b. IP Address/Host: **192.168.10.86**

   c. Health Monitor: leave blank (A Health Monitor is configured in the Service group)



SLB >> Server >> Create

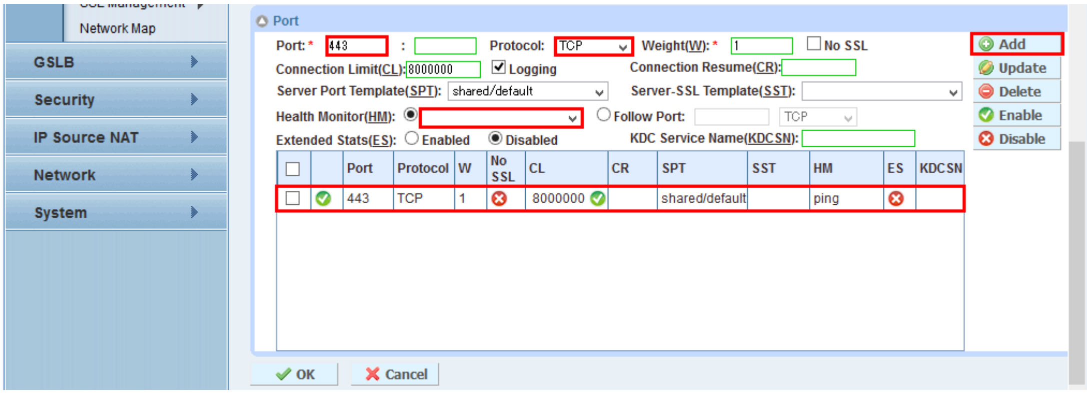
General

Name: *	OWA-Internal-VIP
IP Address/Host: *	192.168.10.86 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□
Firewall:	□
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Server Template:	shared/default

Figure 61: Reverse Proxy server configuration for Office Web Apps Farm

8. Scroll down to the Port section and add port information.

   a. Enter TCP/443, choose blank in Health Monitor (HM), and click **Add**.



Port

Port: * 443 : Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): shared/default Server-SSL Template(SST):

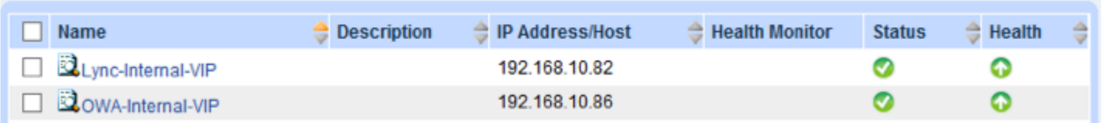
Health Monitor(HM): ● ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	443	TCP	1	✗	8000000 ✓		shared/default		ping	✗	

Figure 62: Reverse Proxy server port configuration for Office Web Apps Farm

9. Click **OK** after the configuration is completed and click **Save** to save the configuration.



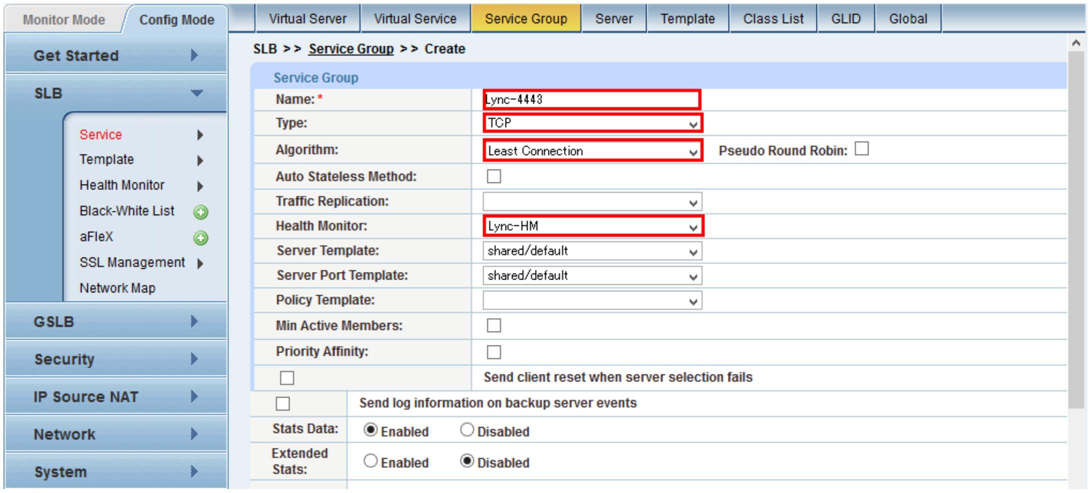
□	Name	Description	IP Address/Host	Health Monitor	Status	Health
□	Lync-Internal-VIP		192.168.10.82		✓	●
□	OWA-Internal-VIP		192.168.10.86		✓	●

Figure 63: Server list for reverse proxy

8.4 Service Group Configuration

Configure a service group for Reverse Proxy.

1. Move to Config Mode >SLB > Service > Service Group.
2. Click Add and create a new service group.
3. Use the following info in this test environment:
   a. Name: Lync-4443
   b. Type: TCP
   c. Algorithm: Least Connection
   d. Health Monitor: **Lync-HM**



SLB >> Service Group >> Create

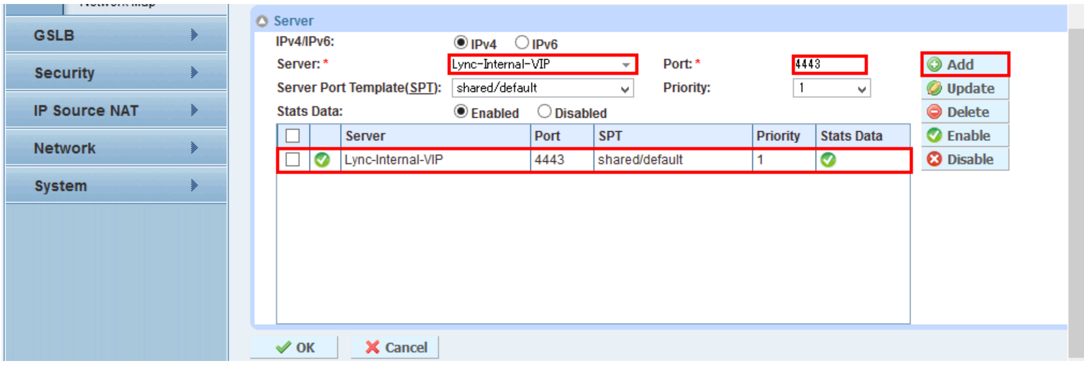
Service Group

Name: *	Lync-4443
Type:	TCP
Algorithm:	Least Connection Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	Lync-HM
Server Template:	shared/default
Server Port Template:	shared/default
Policy Template:	
Min Active Members:	□
Priority Affinity:	□
□	Send client reset when server selection fails
□	Send log information on backup server events
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled

Figure 64: Reverse Proxy service group configuration for Lync Server 2013 Front End pool

Note: The set of real server, port and server selection algorithm are defined in a service group.

4. Choose Lync-Internal-VIP as the Server, set 4443 in Port, and click Add.



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * Lync-Internal-VIP   Port: * 4443

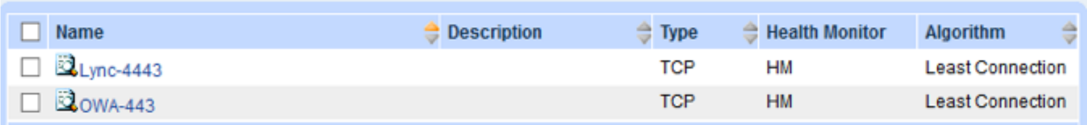
Server Port Template(SPT): shared/default   Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	Lync-Internal-VIP	4443	shared/default	1	✓

Figure 65: Reverse Proxy service group port configuration for Lync Server 2013 Front End pool

5. Click OK after the configuration is completed and click Save to save the configuration.
6. Repeat the above steps (from 1 to 4) to configure a reverse proxy service group for Office Web Apps farm. In this test environment, the following input is used:
   a. Name: OWA-443
   b. Type: TCP
   c. Algorithm: Least Connection
   d. Health Monitor: Lync-HM
   e. Port: 443



□	Name	Description	Type	Health Monitor	Algorithm
□	Lync-4443		TCP	HM	Least Connection
□	OWA-443		TCP	HM	Least Connection

Figure 66: Service Group list for Reverse Proxy

8.5 Virtual Service Configuration

Configure a virtual server and a virtual service for Reverse Proxy in the virtual service configuration.

1. Move to Config Mode > SLB > Service > Virtual Service.
2. Click Add and then create a Virtual Service for Reverse Proxy, In this test environment, the following input is used:

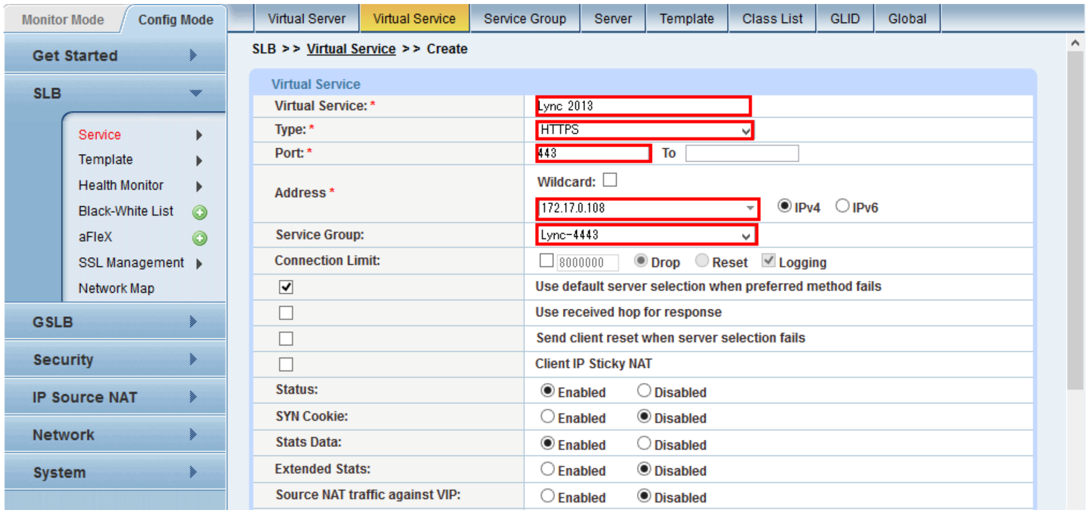
   a. Virtual Service: Lync 2013

   b. Type: HTTPS

   c. Port: 443

   d. Address: 172.17.0.108

   e. Service Group: Lync-4443



SLB >> Virtual Service >> Create

Virtual Service

Virtual Service:*	Lync 2013
Type:*	HTTPS
Port:*	443 To
Address*	Wildcard: □ 172.17.0.108 ● IPv4 ○ IPv6
Service Group:	Lync-4443
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled

Figure 67: Reverse Proxy virtual service configuration

3. In this test environment, the following input is used to configure a feature template:

   a. Source NAT Pool: Auto

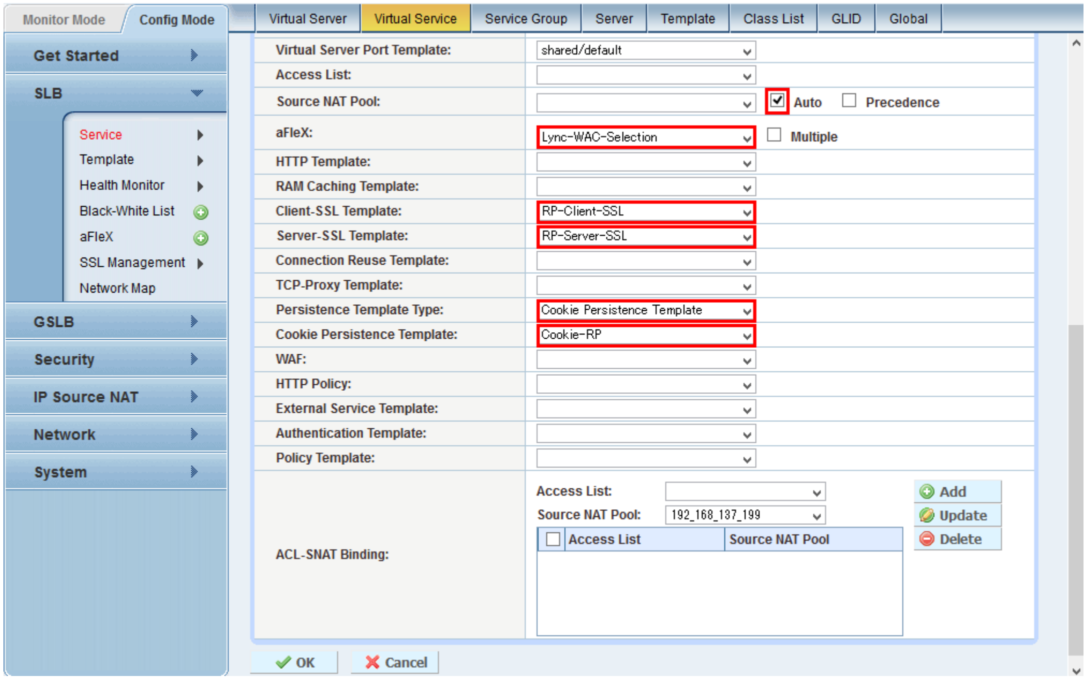
   b. aFleX: Lync-WAC-Selection (Detail is provided in Section 8.6)

   c. Client SSL Template: RP-Client-SSL

   d. Server SSL Template: RP-Server-SSL

   e. Persistence Template Type: Cookie Persistence Template

   f. Cookie Persistence Template: Cookie-RP
   (This setting is similar to the cookie template persistence used in Office Web Apps)



Virtual Server Port Template: shared/default
Access List:
Source NAT Pool: ☑ Auto ☐ Precedence
aFleX: Lync-WAC-Selection ☐ Multiple
HTTP Template:
RAM Caching Template:
Client-SSL Template: RP-Client-SSL
Server-SSL Template: RP-Server-SSL
Connection Reuse Template:
TCP-Proxy Template:
Persistence Template Type: Cookie Persistence Template
Cookie Persistence Template: Cookie-RP
WAF:
HTTP Policy:
External Service Template:
Authentication Template:
Policy Template:
ACL-SNAT Binding:
Access List:
Source NAT Pool: 192_168_137_199

☐ Access List	Source NAT Pool

Figure 68: Feature template configuration for Reverse Proxy virtual service

Note: *To use the same VIP for published Lync Server 2013 and Office Web Apps, FQDN and URL based traffic distribution has to be configured and an aFleX script is used in conjunction in this test environment. The same thing can be carried out with App Switching feature under HTTP template.*

4. Click OK after the configuration is completed and click Save to save the configuration.

8.6 aFleX Configuration

In this test environment, an aFleX Script is used to distribute client access traffic to an appropriate service group based on the URL in the HTTP(S) request header.

1. Move to Config Mode > SLB > aFleX.
2. Click Add
3. In this test environment, the following script is configured to ensure client access to any URL, except wac-hlb.a10domain.a10.com is routed to the Lync-4443 service group and client access to wac-hlb.a10domain.a10.com is routed to OWA-443.

   a. Name: Lync-WAC-Selection

   b. Definition: Set info below.

```
when HTTP_REQUEST {
set FQDN [string tolower [HTTP::host]]
switch $FQDN {
 lync2013.a10domain.a10.com {pool Lync-4443}
   dialin.a10domain.a10.com {pool Lync-4443}
   meet.a10domain.a10.com {pool Lync-4443}
   lyncdiscover.a10domain.a10.com {pool Lync-4443}
   wac-hlb.a10domain.a10.com {
       pool OWA-443
   }
}
}
```

Note: *URL based routing like the above reduces the number of required public (external) IP address.*

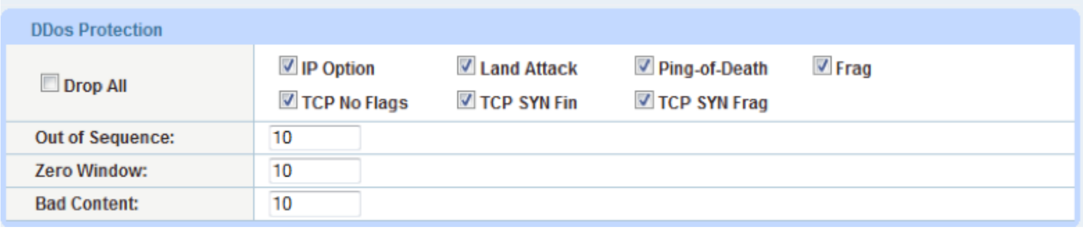
9 Additional Security Features (Optional)

The following section shows additional features that can be implemented within the deployed solution. These features are DDoS Mitigation and Explicit HTTP Proxy.

9.1 DDoS Mitigation

This section describes an additional security feature to protect applications from DDoS attacks. To configure this feature within the ACOS solution, navigate to Config Mode > Security > Network > DDoS Protection.

The DDoS protection feature is a global configuration. To enable this feature, select the necessary DDoS attacks you would like to drop. In Figure 70, we have selected the DDoS attack mitigation required. Once completed, click OK and Save the configuration.



DDos Protection

□ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 69: DDoS protection

In addition, system-wide PBSLB needs to be configured to activate "Out of Sequence," "Zero Window," and "Bad Content" DDoS mitigations. The following two command lines can be used to deploy system-wide PBSLB using the CLI:

```
system pbslb bw-list ddos
system pbslb over-limit lockup 5 logging 10
```

The Black/White list is applied to the system-wide PBSLB within a locking time of 5 minutes and logging interface of 10 minutes.

Note: The sample BW-List contains group ID 1; however, you don't need to configure the group ID in the PBSLB configuration since a wildcard address is used in the list. To use a specific host or subnet address in the list, please configure the action (reset or drop) for each group ID accordingly.

9.2 Explicit HTTP Proxy

One of the most common features of the TMG is to have them act as a Web Proxy Server. This feature enables a client to request resources from a proxy server by enabling/disabling access to websites and services available. This feature is commonly implemented in an enterprise environment to provide control to access unrelated and unnecessary websites or services. This feature can also be integrated with the ACOS Application Access Management (AAM) feature to authenticate clients' access.

You can use the ACOS-powered device as an explicit HTTP proxy to control client access to hosts based on lists of allowed traffic sources (clients) and destinations (hosts). When this feature is enabled, an HTTP virtual port on the ACOS-powered device intercepts HTTP requests from clients, validates both the sources and the destinations, and forwards only those requests that come from valid sources and that are sent to permitted destinations. Destinations are validated based on URL or hostname strings. For approved destinations, DNS is used to obtain the IP addresses.

The destinations requested by clients can be filtered based on the URL of the request or the hostname in the Host header of the HTTP request.

- If both the source and destination are allowed, ACOS translates the client address into a NAT address, if applicable, and forwards the request to the destination.
- If the source or destination is not explicitly allowed by the applicable source or destination list, the request is dropped.

To provide precise control, class lists and a policy template are required to define the source and destination and matching actions for matching traffic. The control mechanism can also be logged based on the request to be permitted, denied (dropped) or DNS failure or SNAT failure.

To configure Explicit Proxy there a few steps:

1. Configure the Ethernet data interface connected to the source and destination

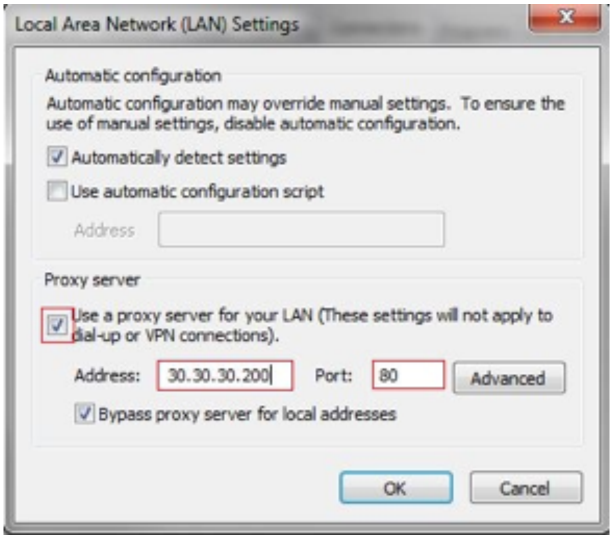
   Note: This configuration has to be done within the internal Lync load balancer so that all external website access are monitored for every internal clients.

2. Specify the DNS server to use for resolving destination IP addresses.
3. Create the class lists:
   - Destinations – String class list that contains the URL or hostname strings for destinations that clients are allowed to access.
   - Sources – IPv4 or IPv6 class list that specifies the client hosts or subnets that are allowed to access the destinations.
   - NAT clients (if applicable) – IPv4 or IPv6 class list that matches on the inside host or subnet addresses that will needed to be NAT-ted.
4. Create a class-list group that matches on the URLs or host names of client requests.
5. If using source NAT, configure the pool and the GLID that refers to it.
6. Create a dummy real server and add it to a service group.
7. If you plan to use a fail-back service group, create the server configurations and service group.
8. Create a policy template.
9. Configure an HTTP virtual port, and bind the following resources to it:
   - Policy template
   - Class list of NAT clients
   - Service group

Note: A dummy (fake) real server and service-group configuration are required for the feature to operate and to provide statistics for permitted traffic (traffic whose LID action is forward-to-internet).

Once configured the browser (tested with Internet Explorer (IE), Mozilla, Chrome) has to be configured to point to the proxy server. Different browser has different set of setting and here is a sample setting for Microsoft IE to configure the proxy server configuration.

On IE navigate to the Menu > Internet Options > Connections tab > LAN Settings > Proxy server.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 30.30.30.200 Port: 80

☑ Bypass proxy server for local addresses

Figure 70: IE proxy server setting

Interface and DNS Server Configuration

Data Interface Configuration:

```
interface ethernet 1
ip address 192.0.2.10 255.255.255.0
!
interface ethernet 2
ip address 203.0.113.46.1 255.255.255.0
```

DNS Server Configuration:

```
ip dns primary 192.168.10.14
```

Class-List Configurati.on

This example shows a class-list to match the destination of a request. All matches are mapped to "lid 1", which will be configured in the policy template. The example below will allow request destined to a string that starts with the presiding letter. Example: "str a lid 1" will allow navigation to a10networks.com.

```
class-list cl-allowed-destinations string
str a lid 1
str b lid 1
str c lid 1
str d lid 1
str e lid 1
str f lid 1
str g lid 1
str h lid 1
str i lid 1
str j lid 1
str k lid 1
str l lid 1
str m lid 1
str n lid 1
str o lid 1
str p lid 1
str q lid 1
str r lid 1
str s lid 1
str t lid 1
str u lid 1
str v lid 1
str w lid 1
str x lid 1
str y lid 1
str z lid 1
```

Class-List Group Configuration

The following commands are used to configure the class-list group, which contains the rules for matching on destinations. This class-list group contains a single rule that matches on host names that contain any string in the string class-list. In this example, any host name that contains at least one English letter will match.

```
class-list-group clg-match-hosts
sequence-number 1 HOST contains cl-allowed-destinations lid 1
```

Source List

The following commands configure the class list that defines the traffic sources (inside clients). In this example, the source is a single host. The host is mapped to "LID 2" in the policy template.

```
class-list cl-allowed-sources ipv4
203.0.113.46.118 /32 lid 2
```

Source NAT Configuration

Command to configure the source that will require source NAT:

```
class-list cl-natted-sources ipv4
203.0.113.118 /32 glid 1
```

Configuration of the NAT Pool and the GLID:

```
ip nat pool snat 192.0.2.83 192.0.2.83 netmask /32
!
glid 1
use-nat-pool snat
```

Dummy Real Server and Service Group

The following commands are used to configure a Dummy Real Server and Service Group for the dummy (fake) real server and add it to a TCP service group. The TCP ports for HTTP (80) and HTTPS (443) are added. The HTTP-proxy virtual port to which the service group is bound will intercept client requests sent to destination ports 80 and 443.

```
slb server rs-fake 203.0.113.46
port 80 tcp
port 443 tcp
!
slb service-group sg-fake tcp
member rs-fake:80
member rs-fake:443
```

Policy Template

The Policy Template configuration and the class-list name command refers to the class list that defines the traffic source.

The class-list group action refers matching traffic to the class-list group that defines the allowed destinations.

```
slb template policy explicit-proxy-policy
class-list name cl-allowed-sources
class-list lid 1
action forward-to-internet sg-fake log
class-list lid 2
class-list-group clg-match-hosts
!
```

HTTP-Proxy Virtual Port

HTTP-proxy Virtual Port configuration that will intercept HTTP request from the clients.

```
slb virtual-server vip3 192.168.83.77
port 8080 http
source-nat class-list cl-natted-sources
service-group sg-fake
template policy explicit-proxy-policy
```

10 Lync Tested Features with A10 Thunder ADC

The following items have been tested to confirm that the Thunder ADC works as a Load Balancer and Reverse Proxy for Lync Server 2013 and Office Web Apps. The failover test was also conducted to verify that the Lync Frontend Servers are redundant in the event that one server fails. All tests passed even if one of Lync Front End servers or Office Web Apps servers went down.

Device Type	Category	Test Descriptions	Test Results
Lync 2013 (Internal access/ Remote access)	Basic	Sign-in	Passed
		Address Book Download	Passed
		Presence Change manually	Passed
	IM	IM between two clients.	Passed
		IM among more than three parties	Passed
		File transfer	Passed
	Voice	Voice call between two clients	Passed
		Voice conference among more than three parties.	Passed
	Video	Video chat between two clients	Passed
	Contents Sharing among three parties	Desktop Sharing	Passed
		Application Sharing	Passed
		PowerPoint Sharing	Passed
		Whiteboard	Passed
	Outlook integration	Missed call history	Passed
		Conversation history	Passed
Lync Web App (Remote Access)	Basic	Sign-in and join Web Conference	Passed
	IM Conference	IM among more than three parties	Passed
		Upload/Download file	Passed
	Voice Conference	Voice conference among more than three parties.	Passed
	Contents Sharing among three parties	Desktop Sharing	Passed
		Application Sharing	Passed
		PowerPoint Sharing	Passed
		Whiteboard	Passed
Lync Mobile for iPhone (Remote Access)	Basic	Sign-in	Passed
		Display Info	Passed
		Presence change manually	Passed
	Address Book	User Search	Passed
	IM	IM between two clients.	Passed
		IM among more than three parties	Passed
	Voice	Voice call between two clients	Passed
	Video	Voice conference among more than three parties.	Passed
		Video chat between two clients	Passed
Lync Mobile for iPad (Remote Access)	Contents Sharing	Desktop Sharing	Passed
		Application Sharing	Passed
		PowerPoint Sharing	Passed

11 Summary and Conclusion

This document describes how to configure Thunder ADC as a Reverse Proxy to support Microsoft Lync 2013 Server and Office Web Apps Server.

Deploying Thunder ADC as a Load Balancer and Reverse Proxy for Microsoft Lync Server 2013 and Office Web Apps offers the following features and benefits:

- Transparent application load sharing.
- High availability for Lync Servers, ensuring users can access Lync applications without disruption.
- Scalability, as the Thunder ADC device transparently load balances multiple Lync Communication servers.
- Higher connection throughput to enhance end user experience.
- Improved server performance due to server offloading, including SSL Offload.
- Protection against web application attacks and online security threats
- Consolidated roles on a single platform through multiple partitions.

Thunder ADC, with its integrated reverse proxy and security features, offers the ideal migration path for ForeFront TMG customers. By provisioning Thunder ADC with its robust set of high availability, acceleration, and security features, organizations can ensure a successful Lync deployment. Thunder ADC offers a cost-effective way for organizations to optimize their Lync deployments and empower employees to connect, communicate, and collaborate with Lync.

For more information about Thunder ADC products, please refer to:

http://www.a10networks.com/products/thunder-application-delivery-controller.php

http://a10networks.com/resources/solutionsheets.php

http://a10networks.com/resources/casestudies.php

Appendix

Here is the configuration data used in an actual test environment.

Lync Server 2013 Front End

```
active-partition P4
vlan 510
 untagged ethernet 5 to 6
 router-interface ve 510
!

interface ve 510
 ip address 192.168.10.85 255.255.255.0
!

ip route 0.0.0.0 /0 192.168.10.88
!

health monitor Lync-HM
!

health monitor WAC-80 interval 30 timeout 10
 method http url GET /hosting/discovery expect wopi-discovery
!

health monitor “SIP 5060”
 method tcp port 5060
!

slb server Lync2013FE1 192.168.10.17
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
   port 80  tcp
       no-ssl
!

slb server Lync2013FE2 192.168.10.18
   disable
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
   port 80  tcp
       no-ssl
!

slb server Lync2013FE3 192.168.10.19
   disable
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
   port 80  tcp
       no-ssl
!

slb server WAC1 192.168.10.23
   port 443  tcp
   port 80  tcp
!

slb server WAC2 192.168.10.24
   port 443  tcp
   port 80  tcp
!

slb service-group Lync2013SG-135 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE2:135
    member Lync2013FE1:135
    member Lync2013FE3:135
!

slb service-group Lync2013SG-443 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:443
    member Lync2013FE2:443
    member Lync2013FE3:443
!

slb service-group Lync2013SG-444 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:444
    member Lync2013FE2:444
    member Lync2013FE3:444
!

slb service-group Lync2013SG-4443 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:4443
    member Lync2013FE2:4443
    member Lync2013FE3:4443
!

slb service-group Lync2013SG-5061 tcp
    method least-connection
    health-check “SIP 5060”
    member Lync2013FE1:5061
    member Lync2013FE2:5061
    member Lync2013FE3:5061
!

slb service-group Lync2013SG-5065 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5065
    member Lync2013FE2:5065
    member Lync2013FE3:5065
!

slb service-group Lync2013SG-5070 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5070
    member Lync2013FE2:5070
    member Lync2013FE3:5070
!

slb service-group Lync2013SG-5071 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5071
    member Lync2013FE2:5071
    member Lync2013FE3:5071
!

slb service-group Lync2013SG-5072 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5072
    member Lync2013FE2:5072
    member Lync2013FE3:5072
!

slb service-group Lync2013SG-5073 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5073
    member Lync2013FE2:5073
    member Lync2013FE3:5073
!

slb service-group Lync2013SG-5075 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5075
    member Lync2013FE2:5075
    member Lync2013FE3:5075
!

slb service-group Lync2013SG-5076 tcp
    method least-connection
    health-check Lync-HM
    member Lync2013FE1:5076
    member Lync2013FE2:5076
    member Lync2013FE3:5076
!

slb service-group WAC-SG-80 tcp
    health-check WAC-80
    member WAC1:80
    member WAC2:80
!

slb template tcp TCP
   idle-timeout 1200
!

slb template client-ssl WAC-C-SSL
   cert OfficeWebApps
   key OfficeWebApps pass-phrase encrypted
/+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!

slb template persist source-ip SIP
!

slb template persist cookie pesistence-wac
!

slb virtual-server Lync2013VIP 192.168.10.82
   port 135  tcp
      source-nat auto
      service-group Lync2013SG-135
      template tcp TCP
      template persist source-ip SIP
   port 443  tcp
      source-nat auto
      service-group Lync2013SG-443
      template tcp TCP
      template persist source-ip SIP
   port 444  tcp
      source-nat auto
      service-group Lync2013SG-444
      template tcp TCP
      template persist source-ip SIP
   port 4443  tcp
      source-nat auto
      service-group Lync2013SG-4443
      template tcp TCP
      template persist source-ip SIP
   port 5061  tcp
      source-nat auto
      service-group Lync2013SG-5061
      template tcp TCP
      template persist source-ip SIP
   port 5065  tcp
      source-nat auto
      service-group Lync2013SG-5065
      template tcp TCP
      template persist source-ip SIP
   port 5070  tcp
      source-nat auto
      service-group Lync2013SG-5070
      template tcp TCP
      template persist source-ip SIP
   port 5071  tcp
      source-nat auto
      service-group Lync2013SG-5071
      template tcp TCP
      template persist source-ip SIP
   port 5072  tcp
      source-nat auto
      service-group Lync2013SG-5072
      template tcp TCP
      template persist source-ip SIP
   port 5073  tcp
      source-nat auto
      service-group Lync2013SG-5073
      template tcp TCP
      template persist source-ip SIP
   port 5075  tcp
      source-nat auto
      service-group Lync2013SG-5075
      template tcp TCP
      template persist source-ip SIP
   port 5076  tcp
      source-nat auto
      service-group Lync2013SG-5076
      template tcp TCP
      template persist source-ip SIP
   port 80  tcp
      name _192.168.10.82_TCP_80
      source-nat auto
      service-group Lync2013SG-80
      template tcp TCP
      template persist source-ip SIP
!
```

```
slb virtual-server OWA_VIP 192.168.10.86
   port 443  https
      source-nat auto
      service-group WAC-SG-80
      template client-ssl WAC-C-SSL
      template persist cookie persistence-wac
!

enable-management service ssh ethernet 5 to 6 ve 510
enable-management service https ethernet 5 to 6 ve 510
!
end
```

Lync Server 2013 Internal Edge

```
active-partition P3
vlan 401
 untagged ethernet 3 to 4
 router-interface ve 401
!

interface ve 401
 ip address 172.19.0.211 255.255.255.0
!

ip route 0.0.0.0 /0 172.19.0.241
!

health monitor HM
!

slb server InternalEdge-1 172.19.0.121
   port 443  tcp
   port 3478  udp
   port 5061  tcp
   port 5062  tcp
!

slb server InternalEdge-2 172.19.0.122
   port 5062  tcp
   port 5061  tcp
   port 3478  udp
   port 443  tcp

!

slb service-group InternalEdge-443 tcp
    method least-connection
    health-check HM
    member InternalEdge-1:443
    member InternalEdge-2:443
!

slb service-group InternalEdge-3478 udp
    method least-connection
    health-check HM
    member InternalEdge-1:3478
    member InternalEdge-2:3478
!


slb service-group InternalEdge-5061 tcp
    method least-connection
    health-check HM
    member InternalEdge-2:5061
    member InternalEdge-1:5061
!

slb service-group InternalEdge-5062 tcp
    method least-connection
    health-check HM
    member InternalEdge-1:5062
    member InternalEdge-2:5062
!

slb template tcp TCP
   idle-timeout 1200
!

slb template persist source-ip SIP
!

slb virtual-server _172.19.0.101_vserver 172.19.0.101
   port 443  tcp
      name Internal-443
      source-nat auto
      service-group InternalEdge-443
      template tcp TCP
      template persist source-ip SIP
   port 3478  udp
      name Internal-3478-UDP
      source-nat auto
      service-group InternalEdge-3478
      template persist source-ip SIP
   port 5061  tcp
      name Internal-5061
      source-nat auto
      service-group InternalEdge-5061
      template tcp TCP
      template persist source-ip SIP
   port 5062  tcp
      name Internal-5062
      source-nat auto
      service-group InternalEdge-5062
      template tcp TCP
      template persist source-ip SIP
 !
end
```

Lync Server 2013 External Edge

```
active-partition P2
vlan 201
 untagged ethernet 1 to 2
 router-interface ve 201
!

interface ve 201
 ip address 172.17.0.211 255.255.255.0
!
ip route 0.0.0.0 /0 172.17.0.254
!

health monitor HM
!

slb server ExternalEdge1-access 172.17.0.21
   port 443  tcp
   port 5061  tcp
!

slb server ExternalEdge2-access 172.17.0.31
   port 5061  tcp
   port 443  tcp
!

slb server ExternalEdge1-web 172.17.0.22
   port 443  tcp
   port 3478  udp
!

slb server ExternalEdge2-web 172.17.0.32
   port 443  tcp
   port 3478  udp
!

slb server ExternalEdge1-av 172.17.0.23
   port 3478  udp
   port 443  udp
!

slb server ExternalEdge2-av 172.17.0.33
   port 3478  udp
   port 443  tcp
   port 443  udp
!

slb service-group ExternalEdge-access-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge1-access:443
    member ExternalEdge2-access:443
!

slb service-group ExternalEdge-access-5061 tcp
```

```
    method least-connection
    health-check HM
    member ExternalEdge1-access:5061
    member ExternalEdge2-access:5061
!

slb service-group ExternalEdge-web-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge2-web:443
    member ExternalEdge1-web:443
!

slb service-group ExternalEdge-av-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge1-av:443
    member ExternalEdge2-av:443
!

slb service-group ExternalEdge-av-3478 udp
    method least-connection
    health-check HM
    member ExternalEdge1-av:443
    member ExternalEdge2-av:443
!

slb template tcp TCP
   idle-timeout 1200
!

slb template persist source-ip SIP
!

slb virtual-server _172.17.0.111_vserver 172.17.0.111
   port 443  tcp
      name ExternalEdge-ac443
      source-nat auto
      service-group ExternalEdge-access-443
      template tcp TCP
      template persist source-ip SIP
!

slb virtual-server _172.17.0.112_vserver 172.17.0.112
   port 443  tcp
      name ExternalEdge-web443
      source-nat auto
      service-group ExternalEdge-web-443
      template tcp TCP
      template persist source-ip SIP
!

slb virtual-server _172.17.0.113_vserver 172.17.0.113
   port 443  tcp
      name ExternalEdge-av443
      service-group ExternalEdge-av-443
      template tcp TCP
      template persist source-ip SIP
   port 3478  udp
      name ExternalEdge-av3478
      service-group ExternalEdge-av-3478
      template persist source-ip SIP
!
end
```

Reverse Proxy

```
active-partition P1
vlan 202
 untagged ethernet 7
 router-interface ve 202
!

vlan 402
 untagged ethernet 8
 router-interface ve 402
!

interface ve 202
 ip address 172.17.0.201 255.255.255.0
!
interface ve 402
 ip address 172.19.0.201 255.255.255.0
!

ip route 0.0.0.0 /0 172.17.0.254
ip route 192.168.10.0 /24 172.19.0.241
ip route 172.18.0.0 /24 172.19.0.241
!

health monitor HM
!

slb template server-ssl RP-Server-SSL
   ca-cert a10domain_a10_local_rootCA
!

slb server Lync-Internal-VIP 192.168.10.82
   port 4443  tcp
!

slb server OWA-Internal-VIP 192.168.10.86
   port 443  tcp
!

slb service-group Lync-4443 tcp
    method least-connection
    health-check HM
    member Lync-Internal-VIP:4443
!

slb service-group OWA-443 tcp
```

```
    method least-connection
    health-check HM
    member OWA-Internal-VIP:443
!

slb template client-ssl RP-Client-SSL
   cert 20131007RP-2
   key 20131007RP-2 pass-phrase encrypted
/+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!

slb template persist source-ip RP
!

slb virtual-server _172.17.0.108_vserver 172.17.0.108
   port 443  https
      name Lync2013
      source-nat auto
      service-group Lync-4443
      template client-ssl RP-Client-SSL
      template server-ssl RP-Server-SSL
      template persist coolie Cookie-RP
      aFleX Lync-WAC-selection
!

enable-management service https ethernet 7 to 8 ve 202 ve 402
!

end
```

Explicit HTTP Proxy Sample Configuration

```
Sample configuration below is a sample configuration for Explicit HTTP Proxy
configuration. The sample configuration does not coincide with the reverse proxy
IP Address scheme so deploy accordingly.
!
class-list cl-allowed-sources ipv4
 30.30.30.20 /32 lid 2
 0.0.0.0 /0 lid 1
!
class-list cl-allowed-destinations string
 str o lid 1
 str g lid 1
 str a lid 1
 str r lid 1
 str x lid 1
 str u lid 1
 str f lid 1
 str m lid 1
 str i lid 1
 str t lid 1
 str w lid 1
 str n lid 1
 str z lid 1
 str j lid 1
 str d lid 1
 str b lid 1
 str h lid 1
 str q lid 1
 str p lid 1
 str l lid 1
 str e lid 1
 str k lid 1
 str v lid 1
 str c lid 1
 str s lid 1
 str y lid 1
!
class-list cl-natted-sources ipv4
 30.30.30.30 /32 glid 1
!
class-list cl-allowed-destination string
 str 10.10.10.10 lid 1
!
class-list-group clg-match-hosts
    sequence-number 1 HOST contains cl-allowed-destinations lid 1
!
ip nat pool p1 10.100.2.150 10.100.2.150 netmask /32
ip nat pool p2 10.10.10.50 10.10.10.50 netmask /32
!
glid 1
 use-nat-pool p2
!
slb template server default
   no health-check
!
slb template port default
   no health-check
!
slb server “IIS Server 1” 10.10.10.10
   port 80  tcp
!
slb server “IIS Server 2” 10.10.10.11
   port 80  tcp
!
slb server rs-fake 45.123.46.86
   port 80  tcp
   port 443  tcp
!
slb service-group sg80 tcp
    member “IIS Server 1”:80
    member “IIS Server 2”:80
!
!
slb service-group sg-fake tcp
    member rs-fake:80
    member rs-fake:443
!
slb template policy explicit-proxy-policy
   class-list name cl-allowed-sources
   class-list lid 1
      class-list-group clg-match-hosts
      action forward-to-internet sg-fake log
   class-list lid 2
      class-list-group clg-match-hosts
!
slb virtual-server IISVIP 30.30.30.200
   port 80  http
      source-nat class-list cl-natted-sources
      service-group sg80
      template policy explicit-proxy-policy
!
ip dns primary 10.100.2.159
ip dns secondary 8.8.8.8
!
```

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16139-EN-01
Aug 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.