



# Thunder ADC with Microsoft Skype for Business Server 2015 Deployments

# List of Figures

-

Overview	
Skype for Business Server 2015 Roles	
Front End Servers	
Back End (BE) Server	5
Edge Server	5
Office Online Server	5
Reverse Proxy	5
Deployment Topology	5
Configuring the Thunder ADC Device	7
Log into the CLI	7
Log onto the GUI	
Services Required for Skype for Business 2015 Deployment	9
Feature and Configuration Templates on Thunder ADC	13
How to Create a TCP Template	13
How to Configure a Health Monitor	14
Load Balancing for Skype Front End Pool	
Server Configuration	
Service Group Configuration	17
Virtual Server Configuration	
External Edge Load Balancing	
Server Configuration	
Service Group Configuration	23
Virtual Server Configuration	
Internal Edge Load Balancing	
Server Configuration	
Service Group Configuration	
Virtual Server Configuration	27
Load Balancing for Office Online Server Farm	
Server Configuration	
Service Group Configuration	
Virtual Server Configuration	
Health Monitor Configuration	
Client SSL Template Configuration	
Cookie Persistence Configuration	
Reverse Proxy	
Importing Certificate	
SSL Template Configuration	
Server Configuration	
Service Group Configuration	
Virtual Server Configuration	
aFleX Scripting Configuration	
Additional Security Feature – DDoS Mitigation (Optional)	
DDoS Mitigation	

Summary	.40
Appendix	.41
Skype Server 2015 Front End	
Skype Server 2015 Internal Edge	
Skype Server 2015 External Edge	
Reverse Proxy	
About A10 Networks	.51

#### 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.

# **Overview**

A10 Networks<sup>®</sup> Thunder<sup>®</sup> ADC line of Application Delivery Controllers provides intelligent load balancing, security, acceleration and optimization for Microsoft Skype for Business Server 2015.

The purpose of this guide is to provide a step-by-step process for deploying A10 Thunder ADC as a load balancer in a Microsoft Skype for Business Server 2015 deployment.

The following topology (Figure 1) is designed to support Skype for Business 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, four A10 Networks vThunder ADCs are used to deploy four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy. The solution can be deployed with virtual or physical appliances in the same way, and you can also configure Application Delivery Partitions (ADPs) to consolidate the four Thunder ADC devices into one or more (physical or virtual) appliances.

For additional Microsoft deployment guides such as Lync Server, Microsoft Exchange and/or SharePoint, please refer to <u>https://www.a10networks.com/resources/deployment-guides</u>.

#### **Skype for Business Server 2015 Roles**

Each server running Skype for Business Server runs one or more server roles. A server role is a defined set of Skype for Business Server functionalities provided by that server. The primary server roles are described below<sup>1</sup>.

#### **Front End Servers**

In Skype for Business Server Enterprise Edition, the Front End Server is the core server role, and runs many basic Skype for Business Server functions.

The Front End Server includes the following:

- User authentication and registration
- · Presence information and contact card exchange
- · Address book services and distribution list expansion
- IM functionality, including multiparty IM conferences
- Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed)
- Application hosting, for both applications included with Skype for Business Server (for example, Conferencing Attendant and Response Group application), and third-party applications
- · Web components to supported web-based tasks such as web scheduler and join launcher
- (Optionally) Archiving, to archive IM communications and meeting content for compliance reasons
- (Optionally if Persistent chat is enabled) Persistent Chat Web Services for Chat Room Management and Persistent Chat Web Services for File Upload/Download
- (Optionally) Monitoring, to collect usage information in the form of call detail records (CDRs) and call error records (CERs), which provide metrics about the quality of the media (audio and video) traversing your network for both Enterprise Voice calls and A/V conferences

A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. Standard Edition servers cannot be pooled, whereas multiple Enterprise Edition Servers can exist in a pool to provide redundancy and scalability.

#### 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 Servers do not run any Skype for Business Server software. The BE server requirement can be implemented with Microsoft SQL Server 2012 or Microsoft SQL Server 2014 – Standard and Enterprise (64-bit edition)<sup>2</sup>.

#### **Edge Server**

Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include: the organization's own users who are currently working offsite; users from federated partner organizations; and outside users who have been invited to join conferences hosted on your Skype for Business Server deployment. Each Edge Server has two network interfaces, external and internal. The external interface accepts connections initiated from the Internet, and the internal interface accepts connections initiated retwork.

#### **Office Online Server**

Office Online Server is the next version of Office Web Apps Server and is used in Skype for Business Server 2015 for sharing and rendering of PowerPoint presentations.

#### **Reverse Proxy**

Reverse Proxy publishes to the Internet the web components of Front End Servers and Office Online Server (00S) services.

# **Deployment Topology**

Figure 1 shows a Skype for Business Server 2015 deployment using Thunder ADCs. It provides the following services:

- Login and Presence Functionality
- · Instant Messaging, including multiparty IM conferences
- Audio/Video Calls
- Desktop Sharing
- PowerPoint Sharing

In this setup, four vThunder ADCs were used to deploy four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy. The solution can be deployed in the same way using either virtual or physical appliances. You can also configure ADPs to consolidate the four Thunder ADCs into one or more (physical or virtual) devices.

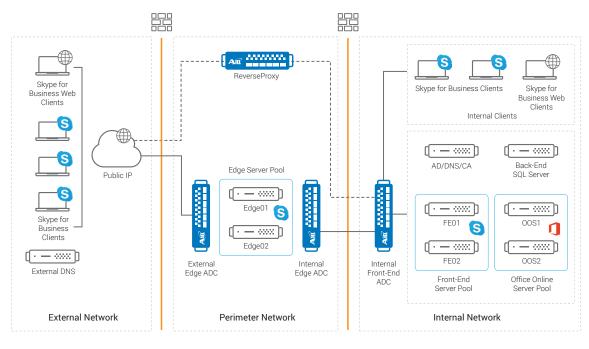


Figure 1: Lab topology

Table 1 shows Hostname and IP address on each element/device used in this guide (as shown in the above diagram).

#### Table 1: Lab Setup

Role	Load Balancing VIP	Device Hostname	IP Address
Active Directory (AD), Internal Certificate Authority (CA), Internal DNS	NA	DC	10.0.3.10/24
Front End	10.0.3.123/24	FE01	10.0.3.12/24
		FE02	10.0.3.13/24
Back End	NA	SQL	10.0.3.11/24
External Edge	192.0.2.111, 112, 113/24	Edge01	192.0.2.21, 22, 23/24
		Edge02	192.0.2.31, 32, 33/24
Internal Edge	10.0.4.30/24	Edge01	10.0.4.31/24
		Edge02	10.0.4.32/24
Office Online Server	10.0.3.125/24	00S1	10.0.3.15/24
(previously Office Web Apps Server)		00S2	10.0.3.16/24
Reverse Proxy	192.0.3.108	Front End VIP	10.0.3.123/24
		OOS VIP	10.0.3.125/25
External DNS	NA	ExternalDNS	198.51.100.10
External Clients (Multiple)	NA	ExternalClient <number></number>	198.51.100.0/24
Internal Clients (Multiple)	NA	InternalClient <number></number>	10.0.2.0/24

Note specific to this guide:

- This setup was tested with A10 Thunder ADC appliances running the A10 Networks Advanced Core Operating System (ACOS<sup>®</sup>) version 4.1.1-P1. The solution was deployed with four vThunder ADC devices, one for each of the four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy. The solution can also be deployed in the same way using virtual or physical appliances, and you can also configure ADPs to consolidate the four Thunder ADC devices into one or more (physical or virtual) appliances. Two devices are going to be required for high availability.
- 2. Microsoft Skype for Business Server 2015 was tested through communication with IM, Presence, Desktop Collaboration and Audio Video (AV) conferencing. Testing was performed for both internal and external users.
- 3. Testing was performed using Microsoft Skype for Business Server 2015 Enterprise Edition Server with 64-bit Microsoft SQL Server 2012 Enterprise Edition.
- Skype for Business 2015 Server Front End and Edge Server components were running on Windows 2012 R2 (64-bit) Standard Edition Server. Office Online Server was running on Windows Server 2012 Datacenter Edition.
- 5. Skype for Business Basic Client 64-bit on Windows 7/10 was used for desktop client.
- 6. Office Online Server (OOS) was tested with PowerPoint presentation sharing.

# **Configuring the Thunder ADC Device**

The Thunder ADC device provides the following management interfaces:

#### Command-Line Interface (CLI)

The CLI is a 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: either of the following protocols: Secure protocol – Secure Shell (SSH) version 2.

Unsecure protocol - Telnet (if enabled)

#### Graphical User Interface (GUI)

The GUI is a 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).

## Log into the CLI

A10 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 has 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 device, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. Click **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:

vThunder>

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 click **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:

vThunder#

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

vThunder (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.

# Log onto the GUI

To log onto the GUI:

1. In your web browser, enter the HTTPS request with the management IP address of the Thunder ADC device, such as https://management-IP-address/. A logon screen is displayed.



Figure 2: GUI login screen

NOTE: For the default admin credentials, the username is admin and the password is a10.

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

The Dashboard page will appear, showing at-a-glance information for your Thunder ADC device.

# Services Required for Skype for Business 2015 Deployment

The following tables list the load-balancing services required for a Skype for Business 2015 Enterprise Server deployment.

#### Table 2: Services on Front End Server

Service Name	Port	vPort Type	Source NAT	Feature Template	Usage Note
Front End Service	135	ТСР	Yes	Persistence: Source-IP TCP: TCP Health Monitor: HM	Used for Distributed Component Object Model (DCOM)-based operations such as Moving Users, User Replicator Synchronization and Address Book Synchronization.
Web Compatibility Service	443	ТСР	Yes	Persistence: Source-IP TCP: TCP Health Monitor: HM	Used for communication from Front End Servers to web farm fully qualified domain names (FQDNs) (the URLs used by IIS web components). Client SSL template is required if SSL offload is configured.
Web Server Component	4443	ТСР	Yes	Persistence: Source-IP TCP: TCP Health Monitor: HM	Used for web access from remote user. Client SSL template is required if SSL offload is configured.
Front End Service	444	TCP	Yes	Persistence: Source-IP TCP: TCP Health Monitor: HM	Used for HTTPS communication between the Focus (Skype for Business 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.
Front End Service	5061	TCP	Yes	Persistence: Source-IP TCP: TCP Health Monitor: HM	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.

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

#### Table 3: Optional Services on Front End Server

**NOTE**: Details of port and protocol Skype for Business 2015 Front End Server uses are described at the following URL: <u>https://technet.microsoft.com/en-us/library/gg398833.aspx</u>

#### Table 4: Services on Internal Edge

Role/ Protocol	Port	vPort Type	Source NAT	Feature Template	Usage Note
STUN/ MSTURN	443	TCP	Yes	Persistence: Source-IP TCP: TCP Health Monitor: 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: Source-IP Health Monitor: HM	Preferred path for A/V media transfer between internal and external users.
Access/SIP	5061	TCP/ MTLS	Yes	Persistence: Source-IP TCP: TCP Health Monitor: 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	ТСР	Yes	Persistence: Source-IP TCP: TCP Health Monitor: 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 Skype for Business 2015 Edge Server uses are described at the following URL: <u>https://technet.microsoft.com/en-us/library/mt346416.aspx</u>

#### Table 5: Services on External Edge

Role/Protocol	Port	vPort Type	Source NAT	Feature Template	Usage Note
Access/ SIP(TLS)	443	ТСР	No (Optional: Yes)	Persistence: Source-IP TCP: TCP Health Monitor: HM	Client-to-server SIP traffic for external user access
Access/ SIP(MTLS)	5061	ТСР	No (Optional: Yes)	Persistence: Source-IP TCP: TCP Health Monitor: HM	SIP signaling, federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)	443	ТСР	No (Optional: Yes)	Persistence: Source-IP TCP: TCP Health Monitor: HM	Web Conferencing media
A/V/ STUN, MSTURN	443	ТСР	No	Persistence: Source-IP TCP: TCP Health Monitor: HM	STUN/TURN negotiation of candidates over TCP/443
A/V/ STUN, MSTURN	3478	UDP	No	Persistence: Source-IP Health Monitor: HM	STUN/TURN negotiation of candidates over UDP/3478

**NOTE**: During feature selection (Figure 3) of the external Edge pool installation, you will be asked to deploy the Skype 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.

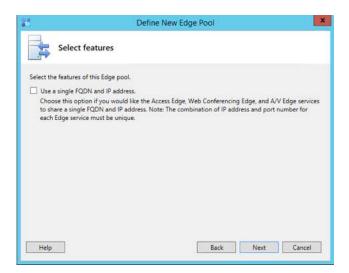


Figure 3: External Edge pool server feature selection

#### **Protocol Definitions**

- 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 6: Service on Office Online Server (Option)

Service Name	Port	vPort Type	Source NAT	Feature Template	Usage Note
Office Online Server Service	443	TCP	Yes	Persistence: Cookie Health Monitor: OOS- 80 Client SSL template: Required	Used for PowerPoint content sharing to Skype for Business clients. SSL Offload is recommended.

#### Table 7: Services on Reverse Proxy (Option)

Service Name	Port	vPort Type	Source NAT	Feature Template	Usage Note
Published Web Service	443 >> 4443 (redirect)	HTTPS	Auto	Health Monitor: HM Client SSL template: Required Server SSL Template: Required A10 Networks aFleX® TCL Scripting Technology or HTTP Template: Required <sup>1</sup>	Used for communication to Skype 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 Online Server Service	443	HTTPS	Auto	Health Monitor: HM Client SSL Template: Required Server SSL Template: Required aFleX TCL Scripting or HTTP Template: Required <sup>1</sup>	Used for PowerPoint content sharing/shared from remote users.

**NOTE**: Details of ports and protocol of Reverse Proxy is described at the following URL: <u>https://technet.microsoft.com/en-us/library/gg615011.aspx</u>

# Feature and Configuration Templates on Thunder ADC

This section describes steps to configure three features templates listed in the table above:

- L4 protocol template with TCP
- Persistence template with Source IP basis
- Health monitor template using ICMP (or TCP)

## How to Create a TCP Template

- 1. Go to ADC > Templates > SLB > L4 Protocols.
- 2. Click Create > TCP and configure as shown below:
  - Name: TCP
  - Idle Timeout: 1800
- 3. Click OK after configuration is completed and click Save to save configuration.

TCP	⊖ Hep
TCP	
ТСР	
TCP	
1800	
Enable      Disable     Dis	
Enable Science Disable	
	© Enable ® Disable © Enable ® Disable © Enable ® Disable © Enable ® Disable

Figure 4: L4 TCP template

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

How to Configure Source IP Persistence

- 1. Go to ADC > Templates > Persistence.
- 2. Click Create > Persist Source IP and configure as shown below:
  - Name: SIP
  - Timeout: 20 Minutes
  - Netmask: 255.255.255.255 (default value)
- 3. Click OK after configuration is completed and click Save to save the configuration.

Create Persist Source IP 1	remplate	O Help
Name *	SIP	
Dont Honor Conn Rules	Sie	
Enforce Higher Priority	8	
Hash Persist		
Include Destination IP		
Include Source Port	0	
Match Type		•
Timeout(minutes)	20	
Netmask	255 255 255 255	
IPv6 Netmask	128	
		Cancel

Figure 5: Source IP persistence template

## How to Configure a Health Monitor

- 1. Go to ADC > Health Monitors > Health Monitor.
- 2. Click **Create** and configure as shown below:
  - Name: HM
  - Use the default value in other fields
- 3. Click OK after completion and click Save to save the configuration.

Monitors External	Programs HTTP Post Files Global Setting	Statistics Galewa	y.				vThunder 4.1.1-P1 bui
> Health Monitors	>> Create						O He
ate Health Mo	nitor						
	General Fields		•			ICMP	0
Name *	HM			Transparent	8		
Method Type	ICMP						
Retry	3						
Up Retry	1						
Interval	6						
Timeout	5						
Override IPv4							
Override IPv6							
Override Port							
SSL Cipher Suite							
Passive							
Strict Retry On Server Err Resp							
Enable Strict L2dsr health-	0						

Figure 6: Health Monitor configuration

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

Name: TCP-443 Interval: 30 Timeout: 10 Type: TCP Port: 443 Half Open: False

# Load Balancing for Skype Front End Pool

One or more pools can be configured in each site, and one or more Skype Front End Servers can be configured in each pool. The Skype Front End Server pool is a core component and composed of one or more Skype Front End Servers. IM/Presence, every Conference service, collaboration and voice are just a few of the services provided by the Front End pool. If there are multiple 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.

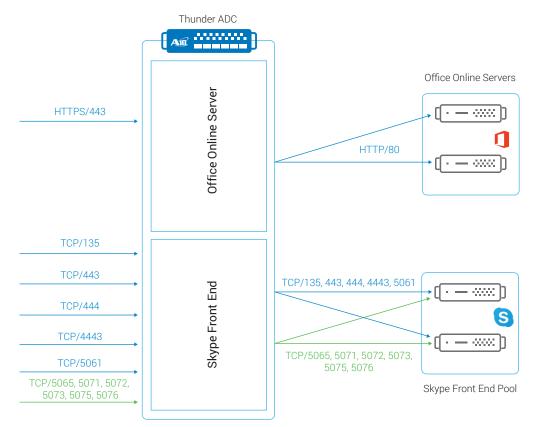


Figure 7: Load balancing image diagram for Front End pool and Office Online Servers

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

## **Server Configuration**

Configure Skype Front End Servers on the Thunder ADC.

- 1. Go to ADC > SLB > Servers.
- 2. Click Create to add a new server. In this test environment, the following information is used:
  - Name: FE1
  - Host: 10.0.3.12
  - Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)

ual Servers Virtual S	ervices Service Groups Servers Policy Limits	Class Lists + Applica	tion Glob	al Session +	Resource	Jsage			vThunder 4.1	
>> SLB >> Serve	rs >> Create									<b>9</b> Hel
reate Server										
Name *	FE1					P	ort			
Туре	IPv4   IPv6   FQDN									Create
Host *	10.0.3.12			Port Protoco	Weight	Conn Limit	Health	Range	Conn Resume	Action
Action	Enable		Noitem	s to display.		Limit	Check		Resume	
Disable Health Check	0			ne disputy.						
Health Monitor		▼ Add+								
Connection Limit	8000000									
No Logging	0									
	Advanced Fields	0								
										-
									Cancel	Greate

Figure 8: Configure a Front End Server

- 3. Click on Create in the Port section.
  - Enter the port number, select a proper protocol type, choose default for other values and click Create.

>> Create	😡 Hel
135	
TCP	•
0	
Default O Disable Monitor O Follow Port	
800000	
8	
Advanced Fields	E
	Cancel Greate
	TCP 0 ® Default © Disable © Monitor © Follow Port 8000000

Figure 9: Configure ports for Front End Server

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

al Servers Virtual S	nvices Service Groups Servers Policy Limits	Class Lists + Applicatio	n Glo	bal S	ension +	Resource (	Jsage		8	vThunder 4.1	.1-P1 build
>> SLB >> Server	s >> Update										<b>O</b> Hel
odate Server											
Name *	FE1						P	ort		_	_
Туре	8 IPv4 9 IPv6 FQDN									Delete	Greate
Host *	10.0.3.12		-	Port	Protocol	Weight	Conn Limit	Health Check	Range	Conn Resume	Action
Action	Enable	•	10	135	tcp	1	8000000	Default	0		Edit
Disable Health Check				443	top	1	8000000	Default	0		Edit
Health Monitor		* Add+		444	tcp	1	8000000	Default	0		Edit
Connection Limit	8000000		12	4443	tcp	1	8000000	Default	0		Edit
No Logging			8	5061	tcp.	t	8000000	Default	0		Edit
			13	5065	tcp	1	8000000	Default	0		Edit
	Advanced Fields	C	10	5070	tcp	1	8000000	Default	0		Edit
			8	5071	tcp	1	8000000	Default	0		Edit
			8	5072	tcp	5	8000000	Default	0		Edit
			10	5073	tcp	1	8000000	Default	0		Edit
			8	5075	tcp	1	8000000	Default	0		Edit
			8	5076	tcp	1	8000000	Default	0		Edit

Figure 10: Configured port list for Front End Server

- 4. Click Update after the configuration is done and click Save to save the configuration.
- 5. Repeat the above steps (from 2 to 4) until all Front End Server configurations are completed. In this guide, FE2 is configured as well.

A	0,	Dashboard -		GSLB -	Security	- AAM - C	GN - Neb	work - Syst	em 🕌				😭 Paret	ion: share	id 🗸 🥹	Language 🛩 🧲	) Showlech 😫	Sayer 📥 adm	in 📑 Sign O
Artual 1	servers	Virtual Service	s Se	ivice Groups	Sen	ers Policy La	nts Clas	is Lists -	Applicat	ton Gio	bill Se	1570n ÷	Resource Usa	ge				vThunder	4.1.7-P1 build
DC >>	SLB >	> Servers																	Help
Nar	ne •	Search			Tags	All v	Search	Reset					CR				-		
						(40) · · · · · · · · · · · · · · · · · · ·	Jeann	Preser					No Re	fresh	× Clear	O Enable	O Disable	Celete	+ Create
-	Cantor	Name	Trees	10.444	0.01			Nesei	Conn	ections		Re	quests	fresh	K Clear Bytes				
	Status	Name	Tags	IP Add	0.01		Monitor	Curren		ections Total	Peak	Re Total		Forwa	Bytes		O Disable Statistics I		+ Create
	Status	Name FE1	Tags	IP Add	iress						Peak 0		quests	Forw	Bytes			Details	

Figure 11: Configured Front End Server list

## **Service Group Configuration**

Configure a Service Group for Skype Front End Servers next.

- 1. Go to ADC > SLB > Service Groups.
- 2. Click Create to create a new Service Group. In this test environment, the following data has been used:
  - Name: 135
  - Type: TCP
  - Algorithm: Least Connection
  - Health Monitor: HM

Name *	135				1	Member	
Protocol	TOP	•					Cites
Algorithm	Least Connection		6	Status	Name	Port	Actions
Strict Select	0		No iter	ms to display			
Health Check Disable	0						
Health Monitor	HM	<ul> <li>Add+</li> </ul>					
	Advanced Fields	D					

Figure 12: Front End Servers Service Group configuration

**NOTE**: The set of real servers, port and server selection algorithms are defined at the Service Group level. Multiple Service Groups can be defined if the application uses multiple ports on a single IP.

3. Click Create in the Member section and add the more than one server with appropriate port number.

		Servers Pol	ky Limits	Class Lists	+ AP	plication	Global	Session	. I	Resource	e Usage			v	munder 4.1	
>> SLB >> Service G	roups >> Update															0
date Service Gro	up															
Name *	135											Member				
Protocol	TCP					•							O Enable	O Disable	Delete	Cier
Algorithm	Least Connection					•	0	Stat	us		Name		Port		Actions	
Strict Select	10						0	0	F	E1		135			Edit	
Health Check Disable	6						10	0	F	E2		135			Edit	
Health Monitor	НМ					<ul> <li>Add+</li> </ul>										
	Adva	nced Fields				0										
															Cancel	Upda
																-

Figure 13: Front End Server Service Group

- 4. Click Update after the configuration is done and click Save to save the configuration.
- 5. Repeat the above steps (from 2 to 4) for all required ports and optional ports, if needed. Please refer to Table 1 and Table 2 to see which ports should be configured.

uat	Servers	Vitual:	Services 1	Service G	conb.e	Servers Policy Lin	oto:: C	Dass Lists +	Applica	ation	Global Set	ision +	Resource	Usage						x Thunder 4	(1.1.P1 build 3
2	> SLB :	> Servi	ice Groups																		O Help
Na	me •	Searth			π	igs Al +	Sean	ch Reset									C Refresh	×c	ear	🗄 Delete	+ Create
			Name			Algorithm		Conne	ctions		Request	ts	Byt	es		3	Servers			tistics	variation
0	Status		Name	Tag	s Typ	Algorithm		Current	Total	Peak	Success	Total	In	Out	Up	Down	Disabled	Total	512	osucs	Actions
8	0	135	8	9	tcp	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charls	Edit
	0	443	6	9.1	tcp	Least Connection		0	68	0	0	0	370KB	306KB	2	0	0	2	Stats	Charts	Edit
8	0	444	9	9	tcp	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
à l	0	4443	9	9	tcp	Least Connection		0	10464	G	0	0	11/8	2MB	2	0	0	2	Stats	Charts	Edit
8	0	5061	8	9.3	tcp	Least Connection		5	1726	G	0	0	3MB	3MB	2	0	0	2	Stats	Charts	Edit
116	0	5065	8	9	top	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
3	0	5070	8	9.1	tcp	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
1	0	5071	8		tcp	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
1	0	5072	8	9	tcp	Least Connection		0	0	0	0	-0	0	0	2	0	Ð	2	Stats	Charts	Edit
	0	5073	9	Э	tcp	Least Connection		0	0	0	0	0	0	0	2	0	D	2	Stats	Charts	Edit
	0	5075	9	9	tcp	Least Connection		0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
	0	5076	8	9	tcp	Least Connection		0	0	0	0	0	0	0	2	0	D	2	Stats	Chatts	Edit

Figure 14: Front End Server Service Group list

## **Virtual Server Configuration**

Next, create a virtual server (also as known as VIP) for Front End services.

- 1. Go to ADC > SLB > Virtual Server.
- 2. Click Create to create a virtual server. In this test environment, the following data is being used:
  - Name: FEVIP
  - IP Address : 10.0.3.123

**NOTE**: Multiple virtual servers can be configured on the Thunder ADC device. 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 the client request to it.

Dasho ual Servers Virtual	Services Service Groups Servers Policy Limits Class Lis	in w Apples	ton Global Session - Response Hanne	vThunder 4.1.1-P1 build
		a Contraction	ani onne onner: retrier onde	
; >> SLB >> Virtu	al Servers >> Create			• Hel
Create Virtual S	erver			
Name *	FEVIP		Α.	Virtual Port
Use-If-Ip	Enable     Since Disable		Port Number	Port Range Protocol Actions
Wildcard Address Type *	IPv4 ◎ IPv6		No items to display	
IP Address * Netmask	10.0.3 123			
Action	Enable	۲		
	Advanced Fields	۵		
				Cancel Greate
				· · · · · · · · · · · · · · · · · · ·

Figure 15: Front End Server virtual server configuration

- 3. Go to the Virtual Port section and click Create to configure a virtual server port.
- 4. In the Virtual Server Port setting section, the test environment inputs the following configuration:
  - Name: \_10.0.3.123\_TCP\_135
  - Protocol: TCP
  - Port: 135
  - Service Group: 135

al Servers Virtual Services Servic	e Groups Servers Policy Limits Class Lists + Application Global Session + Resource Usage	vThunder 4.1.1-P1 buil
>> SLB >> Virtual Servers >> FI	VIP >> Virtual Port >> Create	<b>O</b> He
eate Virtual Port		
Name	_10.0.3.123_TCP_185	
Protocol *	TCP	
Port *	135	
Alternate Port		
Range		
Connection Limit	8000000	
Reset	8	
No Logging	8	
Action	Enable	•
Service Group	135	▼ Add+
	General Fields	1
	Templates	
		Cancel

Figure 16: Front End Server virtual port configuration

- 5. Expand the section General Fields:
  - Source NAT Auto: Enabled

		General Fields		
Use Alternate Port	0			
Def Selection If Pref Failed	Enable      Disable			
HA Conn Mirror				
Reset On Server Selection Fail	0			
ClientIP Sticky Nat	0			
Extended Stats	8			
SNAT On Vip				
Stats Data Action	Enable Obisable			
Syn Cookie	8			
ACL				+ Add
	ACL ID/Name	Source NAT Pool	ACL Sequence Number	Action
	- mp_payrous_spinoe			
aFleX Scripts	logging_clients			<b>^</b>
	🖾 redirect1			
	redirect2			
	redirect_rewrite			*
No Auto Up On aFleX	0			
No Dest NAT	8			
Source NAT Pool				•
Source NAT Auto	8			
Precedence	0			

Figure 17: Front End Server Source NAT configuration

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

- 6. Expand the section templates:
  - Template TCP: TCP
  - Persist Type: Source IP
  - Template Persist Source IP: SIP

Deployment Guide | Thunder ADC with Microsoft Skype for Business Server 2015 Deployments

odate Virtual Port			
Name	10.0.3.123_TCP_135		
Protocol *	tcp		
Port *	135		
Alternate Port			
Range	0		
Connection Limit	800000		
leset	8		
lo Logging	0		
Action	Enable	,	
Service Group	135	*	Add+
	General Fields		
	Templates		
Template Virtual Port		*	Add+
Template TCP	TCP		Add+
Template Policy			Add+
Template Scaleout			
Persist Type	Destination IP     SSL SID     Source IP		
Template Persist Source IP	SIP	,	Add+
		Cancel	Up

Figure 18: Front End Server template configuration

**NOTE**: The requirements of each template and of persistence are described at Services Required for Skype for Business 2015 Deployment. Please refer to Table1 and Table 2.

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

Name * Use-If-Ip	FEVIP Enable * Disable				Virtual Port		uleto Crea
Wildcard	Chable Disable			Port Number	Port Range	Protocol	Actions
Address Type *	IPv4			135	0	tcp	Edit
P Address *	10.0.3.123			443	0	tcp	Edit
Vetmask	The states			444	0	tcp	Edit
Action	Enable	*		4443	0	tcp	Edit
				5061	0	tcp	Edit
	Advanced Fields	0	卣	5065	0	tcp	Edit
			8	5070	0	tcp	Edit
				5071	0	tcp	Edit
			13	5072	0	tcp	Edit
			.8	5073	0	tcp	Edit
				5075	0	tcp	Edit
			10	5076	0	tcp	Edit

Figure 19: Virtual server port list for Front End Server pool

9. Click **Update** in the virtual server configuration section after configuration of all virtual server ports are completed, and then click **Save**.

# **External Edge Load Balancing**

Skype Edge Server allows remote users to access internal Front End Server resources through the enterprise firewall and the DMZ/perimeter network. Remote users can use full Skype functionalities, including IM/Presence, Conference, Collaboration and Enterprise Voice without a VPN connection if the Skype Edge pool is deployed.

The Skype 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.

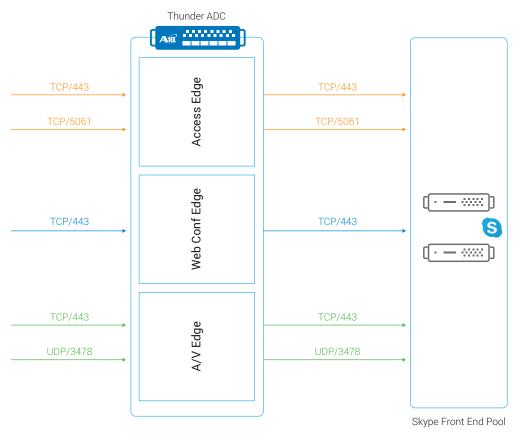


Figure 20: Load balancing image diagram for (external) Edge pool

This section describes how to configure External Skype Edge pool (services) on Thunder ADC.

# **Server Configuration**

Configure Skype External Edge Servers on the Thunder ADC device.

- 1. Go to ADC > SLB > Servers.
- 2. Click Create to create a new server. In this test environment, the following information is used:
  - Name: ExternalEdge1-access
  - Host: 192.0.2.21
  - Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)
- 3. Click on Create in the Port section.
  - Enter the port number, select a proper protocol type, choose default for other values and click Create.
- 4. Repeat the above procedure for all required ports. Refer to Table 4 to determine which ports should be configured.
- 5. Click Update after the configuration is done and click Save to save the configuration.

tual Servers Virtual S	ervices Service Groups	Servers Policy Limits	Class Lists *	Applicate	on Glo	bal S	ession *	Resource	Usage			vThunder 4.1	.1-P1 built
C >> SLB >> Serve	rs >> Update												<b>O</b> He
Jpdate Server													
Name "	ExternalEdge1-access								P	ort			_
Туре	❀ IPv4 ◎ IPv6 ◎ I	FQDN										Delete	Create
Host *	192.0.2.21				8	Port	Protocol	Weight	Conn Limit	Health Check	Range	Conn Resume	Action
Action	Enable				8	443	tcp	1	8000000	Default	0		Edit
Disable Health Check	8					5061		1	8000000	Default	0		Edit
Health Monitor				Add+									
Connection Limit	8000000												
No Logging	0												
	Advanced	d Fields		0									

Figure 21: External Edge Server configuration

**NOTE**: To confirm required ports for the External Skype 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 2 to 5) for all required servers.

tual 2	Servers	Virtual Services Service (	Groups	Servers P	olicy Li	mits Cl	ass Lists 🔻	Application	Glob	al Se	rssion +	Resourc	e Usage				vThunder	1.1.1-P1 buil
C >	> SLB	>> Servers																<b>O</b> He
Na	me •	Search	Tags	All	•	Search	Reset				CR	efresh	× Clear	O Enable	00	sable	💼 Delete	+ Create
		<i>2</i>		10.044				Con	nection		Re	quests		Bytes				
8	Status	Name	Tags	IP Addre	885	Healt	n Monitor	Current	Total	Peak	Total	Success	Forv	ard Recei	ive	Statist	ics Details	Actions
8	0	ExternalEdge1-access		192.0.2.21	æ	Default		2	0	0	0		0	0	0	Stat	s Charts	Edit
0	0	ExternalEdge1-av		192.0.2.23	⊞	Default		0	0	0	0		0	0	0	State	s Charts	Edit
8	0	ExternalEdge1-web		192.0.2.22	Ð	Default		0	0	0	0		0	0	0	Stat	s Charts	Edit
8	0	ExternalEdge2-access		192.0.2.31	æ	Default		1	0	0	0		0	0	0	State	s Charts	Edit
13	0	ExternalEdge2-av		192.0.2.33	Ð	Default		0	0	0	0		0	0	0	State	s Charts	Edit
0	0	ExternalEdge2-web		192.0.2.32	۲	Default		0	0	0	0		0	0	0	Stat	s Charts	Edit
																Total 6	items, Items	or nano: 25

Figure 22: External Edge Server list

## **Service Group Configuration**

Next, create a Service Group for External Edge Servers on the Thunder ADC device.

- 1. Go to ADC > SLB > Service Groups.
- 2. Click Create to create a new Service Group. In this test environment, the following data is being used:
  - Name: ExternalEdge-access-443
  - Type: TCP
  - Algorithm: Least Connection
  - Health Monitor: HM
- 3. Click Create in the Member section and add the more than one server with appropriate port number.
- 4. Click Update after the configuration is done and click Save to save the configuration.
- 5. Repeat the above steps (from 2 to 4) for all required ports and optional ports, if needed. Please refer to Table 4 to determine which ports should be configured.

tual.	Servers	Virtual Services Service Gr	roups	Servers	Policy Limits Citas	is Lists +	Application	Ģ	lobal Sess	sion +	Res	ource U	sage				VT	hunder 4	1.1-P1 build
¢	> SLB	>> Service Groups																	<b>O</b> Hel
N	ame 🗸	Search	Tags	All	• Search	Reset								C Refr	esh	× Clear		Delote	+ Create
8		100 m	12			Con	nections		Request	8	Byt	es		Sen	/ers			100	1.2
10	Status	Name	1	ags Type	Algorithm	Current	Total P	Peak	Success 1	Total	In	Out	Up	Down D	isabled	Total	Sta	tistics	Actions
8	0	ExternalEdge-access-443	æ	tcp	Least Connection	3	0	Ð	0	0	38KB	33KB	2	0	0	2	Stats	Charts	Edit
Ð	0	ExternalEdge-access-5061	田	tcp	Least Connection	0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
8	0	ExternalEdge-av-3478	œ	udp	Least Connection	0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit
0	0	ExternalEdge-av-443	æ	tcp	Least Connection	0	0	Ð	0	0	0	0	2	0	Ð	2	Stats	Charts	Edit
63	0	ExternalEdge-web-443	œ	tcp	Least Connection	0	0	0	0	0	0	0	2	0	0	2	Stats	Charts	Edit

Figure 23: External Edge Server Service Group list

# **Virtual Server Configuration**

Perform the following steps to create virtual servers for External Edge services. In this test environment, the IP Address for each Edge role is independent, so the following steps need to be done for Web Conf and A/V Edge as well:

- 1. Go to ADC > SLB > Virtual Server.
- 2. Click Create to create a virtual server. In this test environment, the following data is being used:
  - Name: \_192.0.2.111\_vserver
  - IP Address: 192.0.2.111
- 3. Go to the Virtual Port section and click Create to configure a virtual server port.
- 4. In the Virtual Server Port setting section, use the following data:
  - Protocol: TCP
  - Port: 443
  - Service Group: ExternalEdge-access-443
- 5. Expand the section templates:
  - Template TCP: TCP
  - Persist Type: Source IP
  - Template Persist Source IP: SIP
- 6. Click Update after the configuration is completed and click Save.
- 7. Repeat the above steps (from 3 to 6) for all required and optional ports. Please refer to Table 4 to determine which ports, templates and persistence should be configured.
- 8. Click Update after the virtual server configuration is completed, and then click Save.
- 9. Repeat the above steps for other virtual servers.

nd Se	ervers 1	Artual Services Service Gro	ops	Servers	Policy	Lints Cla	esa Lista 💌	Application	Global	Sessie	on = Reso	urce Usage				vThunder	4.1.1-P1 buil
55	SLB >>	Virtual Servers															<b>O</b> He
Nam	e• S	sarch	Tags	All	•	Search	Reset				C Refresh	× Clear	0	Enable	00	isable 📋 Delete	+ Create
								Con	nections		Re	quests		Bytes			
3	Status	Name			Tags	IP Add	ress	Current	Total	Peak	Succes	s Tot	al	In Ou	ıt	Statistics	Actions
Э	0	_192.0.2.111_vserver		Β		192.0.2.111		3	0		0	0	0	0	0	Stats Charts	Edit
	0	443_tcp						3	0	1	0	0	0	0	0	Stats	Edit
3.	0	_192.0.2.112_vserver		8		192.0.2.112		0	0	()	0	0	0	0	0	Stats Charts	Edit
	0	443_tcp						Ű	0	1 11	0	0	0	0	0	Stats	Edit
	0	_192.0.2.113_vserver		8		192.0.2.113		0	0		0	0	0	0	0	Stats Charts	Edit
	0	443_tcp						0	0	11	0	0	0	0	0	Stats	Edit
	0	3478_udp						0	0		0	0	0	0	0	Stats	Edit

Figure 24: Virtual Server configuration for External Access, Web Conf and A/V Edge Servers

# **Internal Edge Load Balancing**

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

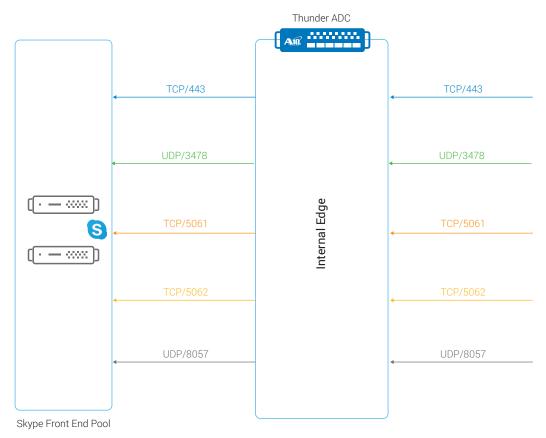


Figure 25: Load balancing image diagram for internal Skype Edge pool

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

#### **Server Configuration**

Create an Internal Edge Server on Thunder ADC.

- 1. Go to ADC > SLB > Servers.
- 2. Click Create to create a new server. In this test environment, the following information is used:
  - Name: InternalEdge-1
  - Host: 10.0.4.31
  - · Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)
- 3. Click on Create in the Port section.
- 4. Enter the port number, select a proper protocol type, choose default for other values and click Create.
- 5. Repeat the above procedure for all required ports. Refer to Table 3 to determine which ports should be configured.
- 6. Click Update after the configuration is done and then click Save to save the configuration.
- 7. Repeat the above steps (from 2 to 6) until all Edge Server configurations are complete. In this test environment, two Edge Servers are being configured.

	Servers	Virtual Services	Service Gro	ups 5	ervers	Policy Linuts Class	Lista = App	ication	Global	Sess	ion - Resid	ace Usage			vThunder	4.1.1-P1 built
2	> SLB	>> Servers														<b>O</b> He
Na	me •	Search		Tags	All	* Search	Reset				C Refresh	X Clear	O Enable	O Disable	Delete	+ Create
a:		1000000	-	-			Con	nections	i.	R	equests	B	/tes			-
1	Status	Name	Tags	IP Ad	idress	Health Monitor	Current	Total	Peak	Total	Success	Forward	Receive	Statisti	cs Details	Actions
9	0	InternalEdge-1		10.0.4.3	1 🕀	Default	0	0	0	(	0 0		0 1	0 Stats	Charts	Edit
	0	tep		443			0	0	0	S (	0	a	0 0	0 (5	itats	
	0	udp		3478			0	0	0		0	() ()	0 0	o s	itats	
	0	tcp		5061			0	0	0	(	0 0	1	0 0	0 5	itats	
	0	tcp		5062			0	0	0		0 0		0 (	0 s	tats	
9	0	InternalEdge-2		10.0.4.3	2 8	Default	0	0	0	0	0 0	1	0 (	0 Stats	Charts	Edit
	0	tcp		443			0	0	0		0	1	0 (	0 s	itats	
	0	udp		3478			0	Ð	0	0	. 0		0	0 8	itats	
	0	top		5061			0	0	0		0	1	0 0	0 s	Rats	
	0	tcp		5062			0	0	0		0		0 1	0 5	tats	

Figure 26: Internal Edge Server list

# Service Group Configuration

Next, create a Service Group for internal Edge servers on Thunder ADC.

- 1. Go to ADC > SLB > Service Groups.
- 2. Click Create to create a new Service Group. In this test environment, the following data is being used:
  - Name: InternalEdge-443
  - Type: TCP
  - Algorithm: Least Connection
  - Health Monitor: HM
- 3. Click Create in the Member section and add the more than one server with appropriate port number.
- 4. Click **Update** after the configuration is done and click **Save** to save the configuration.
- 5. Repeat the above steps for all required service groups with appropriate port list. Refer to Table 3 to determine which Service Groups should be configured.

traii :	Servers	Virtual Services 5	Service G	iroups	Serve	rs Policy I	Limits C	ass Lists +	Applic	ation	Global Se	ssion +	F	despu	itce U	sa)e				vThunder 4	1.1-P1 build
5.0	> SLB	>> Service Groups																			O Hel
Na	me •	Search		Tag	s Al	•	Search	Reset									C Refresh	× Cle	ar	🛱 Delete	+ Create
		722		12		1.52		Con	nection	5	Reques	ts	By	tes			Servers				15.17
13	Status	Name		Tags	Туре	Algor	rithm	Current	Total	Peak	Success	Total	In	Out	Up	Down	Disabled	Total	St	atistics	Actions
0	0	InternalEdge-3478	Θ		udp	Least Conn	ection	0	0	0	0	0	0	0	2	0	0	2	State	s Charts	Edit
	0	InternalEdge-1		3478				0	0	0	D	0	0	0						Stats	
	0	InternalEdge-2		3478				0	0	0	0	0	0	0						Stats	
	0	InternalEdge-443	8		tcp	Least Conn	ection	0	0	0	0		0	10	2	0	0	2	State	Charls	Edit
	0	InternalEdge-1		443				0	0	0	0	0	0	0						Stats	
	0	InternalEdge-2		443				0	0	0	0	0	0	0						Stats	
0	0	InternalEdge-5061	Θ		tcp	Least Conn	ection.	0	.0	.0	0	0	0	0	2	0	) 0	2	Stats	s Charts	Edit
	0	InternalEdge-1		5061				0	0	0	0	0	0	G						Stats	
	0	InternalEdge-2		5061				0	0	0	0	0	0	0						Stats	
	0	InternalEdge-5062	8		tcp	Least Conn	ection	0	0	0	0	0	0	0	2	0	0	2	State	s Charls	Edit
	0	InternalEdge-1		5062				0	0	0	0	0	0	0						Stats	
	0	InternalEdge-2		5062				0	0	0	0	0	0	0						Stats	

Figure 27: Internal Edge Service Group list

# **Virtual Server Configuration**

Perform the following steps to create a virtual server for internal Edge services.

- 1. Go to ADC > SLB > Virtual Server.
- 2. Click Create to create a virtual server. In this test environment, the following data is being used:
  - Name: IEVIP
  - IP Address: 10.0.4.30
- 3. Go to the Virtual Port section and click Create to configure a virtual server port.
- 4. In the Virtual Server Port setting section for this test environment, the following input was used:
  - Name: Internal-443
  - Protocol: TCP
  - Port: 443
  - Service Group: InternalEdge-443
- 5. Expand the section General Fields:
  - Source NAT Auto: Enabled
- 6. Expand the section Templates:
  - Template TCP: TCP
  - Persist Type: Source IP
  - Template Persist Source IP: SIP
- 7. Click Update after the configuration is completed and then click Save.

tual Servers Virtual S	envices Service Groups Servers Policy Limits Class Lists +	Application GR	obal (S	+ noizes	Resource Usage			vThur	nder 4.1.1-P1 build :
C >> SLB >> Virtual	Servers >> Update								O Help
Jpdate Virtual Se	rver								
Name *	OOS-VIP						Virtual Port	_	
Use-If-Ip	Enable 🕐 Disable							and the second se	Delete Contaile
Wildcard			0	443	Port Number	0	Port Range	Protocol	Actions
Address Type *	* IPv4					4.		ingra	Carles 1
IP Address * Netmask	10.0.3.125								
Action	Enable								
	Advanced Fields	D							

Figure 28: Virtual port configuration for internal Edge

- Repeat the above steps (from 3 to 7) for other services (UDP/3478, TCP/5061, TCP/5062). Feature templates are common except UDP/3478. The following input is used for a virtual service with UDP/3478:
  - Name: Internal-3478-UDP
  - Protocol: UDP
  - Port: 3478
  - Service Group: InternalEdge-3478
  - Source NAT Pool: Auto
  - Source IP Persistence: SIP

al S	ervers V	Artual Services Service C	iroups Serve	rs Policy	Limits Cla	ns Lists =	Application	Global	Sessi	on + Reso	urce Usag	e				vThunder	4.1.1-P1 build
>>	SLB >>	Virtual Servers															<b>O</b> Help
Nan	ne 🕶 🛛 Se	earch	Tags All	,	Search	Reset				C Refresh	× Clear		O Ena	ble	O Disable	Delete	+ Create
	Status	Name		Tags	ID Add	IP Address	Con	nections		Re	quests		B	ytes	Stati	ation	Actions
-	outus	Peanlo		19/19	IF Add	055	Current	Total	Peak	Succes	is T	otal	In	Out	3440	5005	Actions
ġ.	0	IEVIP	Ξ		10.0.4.30		0	0		0	0	0	0 0	0	) Stats (	Charts	Edit
	0	443_tcp					0	0		0	0	0	0 0	(	) St	ats	Edit
	0	3478_udp					0	0		0	0	0	0 0	(	) St	ats	Edit
	0	5061_tcp					0	0		0	0	0	0 0		) Sta	its	Edit
	0	5062_tcp					0	0		0	0		0 0		) Sta		Edit

Figure 29: Virtual server configuration for internal Edge pool

# Load Balancing for Office Online Server Farm

Office Online Server (OOS) is the successor to Office Web Apps Server 2013. With Skype for Business Server 2015, OOS enables high fidelity viewing of PowerPoint Online when sharing PowerPoint presentations during meetings.

This section describes how to configure load balancing for an OOS farm on Thunder ADC. SSL offload configuration is recommended for Office Online Server according to the Microsoft Tech Net site<sup>3</sup>.

Additionally, other server offload templates (compression, RAM caching, connection reuse, etc.) on Thunder ADC would be effective for it as well.

An image diagram illustrating load balancing for OOS is shown in Figure 7.

## **Server Configuration**

Add an Office Online Server on Thunder ADC.

- 1. Go to ADC > SLB > Servers.
- 2. Click Create to create a new server. In this test environment, the following information is used:
  - Name: 00S1
  - Host: 10.0.3.15
  - Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)
- 3. Click on Create in the Port section:
  - Port Number: 80
  - Protocol: TCP
- 4. Click Create.
- 5. Click **Update** after the configuration is done, and then click **Save** to save the configuration.
- 6. Repeat the above steps (from 2 to 5) to add additional OOS. In this test environment, two Office Online Servers are configured.

0	0	0051	10.0.3.15	Default	0	.45	0	0	0	29KB	5MB	Stats Charts	Edit
	0	tcp	80		0	- 45	0	0	0	29KB	5MB	Stats	
8	0	OOS2	10.0.3.16	🖯 Default	0	45	0	0	0	29KB	5MB	Stats Charts	Edit
	0	tep	80		0	45	0	0	0	29KB	5MB	Stats	

Figure 30: Office Online Server list

## **Service Group Configuration**

Next, configure a Service Group for the Office Online Server farm on Thunder ADC.

- 1. Go to ADC > SLB > Service Groups.
- 2. Click Create to create a new Service Group. In this test environment, the following data is being used:
  - Name: 00S-SG-80
  - Type: TCP
  - Algorithm: Least Connection
  - Health Monitor: OOS-80 (detail is provided in the Health Monitor Configuration section)
- 3. Click **Create** under the Member section and add servers with the appropriate port number. In this test environment, OOS1 and OOS2 are added with port number 80.
- 4. Click Update after the configuration is done, and then click Save.

Idual Servers Vidual Serv	ces Service Groups	Servers Policy Limbs	Class Lists -	Application	Global	Session +	Resource	Usage			v	Thunder 4.1.1-	P1 build 2
$\rm MC\ggSLB\ggServiceG$	roups >> Update												O Help
Jpdate Service Gro	up												
Name *	00S-SG-80								Membe	t			
Protocol	TCP									O Enable	O Disable	Delefe	Create
Algorithm	Least Connection				0	Status		Name		Port		Actions	
Strict Select	0				13	0	00S1		80			Edit	
Health Check Disable	0					0	0052		80			Edit	
Health Monitor	005-80			• Add+									
	- Arbura	nced Fields		0									

Figure 31: Server list in Office Online Service Group

#### **Virtual Server Configuration**

Configure a virtual server for the Office Online Server farm.

- 1. Go to ADC > SLB > Virtual Server.
- 2. Click Create to create a virtual server. In this test environment, the following data is being used:
  - Name: OOS-VIP
  - IP Address: 10.0.3.125
- 3. Go to the Virtual Port section and click Create to configure a virtual server port.
- 4. In the Virtual Server Port setting section, the following data has been used for this test environment:
  - Name: OOS-VIP\_443\_https
  - Protocol: HTTPS
  - Port: 443
  - Service Group: OOS-SG-80
- 5. Expand the section General Fields:
  - Source NAT Auto: Enabled
- 6. Expand the section Templates:
  - Template Client SSL: OOS-HLB-CSSL (detail is provided in the Client SSL Template section)
  - Persist Type: Cookie
  - Template Persist Cookie: PERSISTENCE-OOS (detail is provided in Cookie Persistence section)
- 7. Click Update after the configuration is done, and then click Save.

A10,		ADC - GSL8 -	Security -	AAM - CG	iN - Network -	System -				🖶 Partition	: shared :	🗸 🥥 Language 🗸	C showlech Save 1	admin 🔁 Sign Out
Virtual Servers	Virtual Services	Service Group	s Servers	Policy Lim	es Class Lists	<ul> <li>Application</li> </ul>	Giobal	1/	ssion +	Resource Usage			vThu	inder 4.1.1-P1 build 38
ADC >> SLB	>> Virtual Serve	rs >> Update												O Help
Update Vi	rtual Server													
Name *		OOS-VIP										Virtual Port		
Use-INp		Enable ® Di	sable					0		Port Number		Port Range	Protocol	Actions
Wildcard Address Ty		<ul> <li>IPv4</li> </ul>							443	Port Homber	0	Fort (tange	https	Edit
IP Address Netmask	e <sup>r</sup>	10.0.3 125												
Action		Enable				٠								
		Ad	Ivanced Fiel	ds			0							
													C	ancel Update

Figure 32: Virtual server configuration for Office Online Server farm

	Templates	
emplate Virtual Port		↓ Add+
emplate Policy		▼ Add+
mplate Scaleout		•
mplate Connection Reuse		*   Add+
mplate Client SSL	OOS-HLB-CSSL	+ Add+
mplate Cache		▼ Add+
nplate TCP Proxy Client		• Add+
mplate HTTP		• Add+
nplate WAF		
mplate TCP Proxy Server		+ Add+
nplate External Service		Add+
nplate HTTP Policy		( <b>•</b> )
nplate Server 5si		
nplate TCP Proxy		• Add+
nplate Dynamic Service		• Add+
rsist Type	10 Destination IP 10 Source IP 🕷 Cookie	
mplate Persist Cookie	PERSISTENCE-OOS	• Add+
mplate REQMOD		Add+
mplate RESPMOD		+ Add+

Figure 33: Template configuration for Office Online virtual service

# **Health Monitor Configuration**

This section describes how to configure a Health Monitor for an OOS Service Group. The Office Online Server returns "wopi-discovery" if a proper GET request comes to the "/hosting/discovery" URI on OOS. You can use this process to create a Health Monitor.

- 1. Go to ADC > Health Monitors.
- 2. Click **Create** to create a new Health Monitor for Office Online Servers. In this test environment, the following data has been used:
  - Name: 00S-80
  - Method Type: HTTP
  - Interval: 30
  - Timeout: 10
  - HTTP Port: 80
  - URL Type: GET
  - URL Path: /hosting/discovery
  - HTTP Expect: HTTP Text
  - HTTP Text: wopi-discovery
- 3. Click Update after the configuration is completed, and then click Save to save the configuration.

**NOTE**: Both Interval and Timeout values depend on the service level in the actual environment. Please ask the IT management department if you need guidance about this.

Monitors External P	rograms HTTP Post Files Global Setting Statist	ica catarinay			vThunder 4.1.1-P1 b
<ul> <li>Health Monitors &gt;&gt;</li> </ul>	Update				0
ate Health Moni	tor				
	General Fields	0		нттр	
Name *	005-80		Specify URL String	2	
Method Type	HTTP		URL Type	GET	*
Retry	3		URL Path	/hosting/discovery	
Up Retry	1		HTTP Host		
Interval	30		HTTP Port	80	
Timeout	10		Maintenance Code		
Override IPv4			HTTP Expect	HTTP Text	Ψ.
Override IPv6			HTTP Text	wopi-discovery	
Override Port			Kerberos Auth		
SSL Cipher Suite	DEFAULT		Usemame		
Passive	0		Password		
Strict Retry On Server Err Resp	Ð				
Enable Strict L2dsr health-check	G				

Figure 34: Health Monitor configuration for Office Online Servers

## **Client SSL Template Configuration**

This section describes how to configure a client SSL template for SSL offload for Office Online Servers.

First, import the certificate for OOS. Usually it is issued by an internal enterprise CA.

- 1. Go to ADC > SSL Management > SSL Certificates.
- 2. Click Import.
- 3. In this test environment, the following data is being used:
  - File Name: OOSCert
  - Import: Certificate
  - Import Certificate from: Local
  - SSL or CA Certificate: SSL Certificate
  - Certificate Format: PFX
  - PFX Password: Actual password for secret key filed with certificate
  - Certificate Source: Actual SSL Server Certificate filename

And Dashboard - ADC -	GSLB + Security + AAM + CGN + Network + System +	📽 Partition: shared 🗸 🧔 🗸 🌘 🤮 💩 admin 🕞
SSL Certificates Cert Revocation List	Expration Email	vThunder 4.1.1-P1 build 38
DC >> SSL Management >> SSL Ce	rtificates >>> Import	G Help
Import SSL Certificate		
File Name *	OOSCert	
Import *	Certificate	
Import Certificate from *	🖲 Local 🔘 Remote 🔘 Text	
SSL or CA Certificate *	SSL Certificate	
Certificate Format	PFX	*
PFX Password	Farman (	
Certificate Source *	Choose File OOSCert.pfx	
Overwrite Existing File		
		Cancel

Figure 35: Import Office Online Server certificate

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

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

- 1. Go to ADC > Templates > SSL.
- Click Create > Client SSL to create a new client SSL template. In this test environment, the following data is being used:
  - Name: OOS-HLB-CSSL
  - Chain Certificate: OOSCert (This is optional)
  - Server Certificate: OOSCert
  - Server Private Key: OOSCert
  - Server Private Key Password Phrase: Password for secret key
- 3. Click OK after the configuration is completed, and then click Save.

**NOTE**: The Server Private Key Name will be different from the Certificate Name if the secret key isn't stored within the certificate file but has been imported separately.

Danhbourd +: ADC + GSLB + Second		and the second second		YPartitions shared ← Q Language		
	NUCLES SE GOURD				sm	under 4
mpianes >> SSL						
						0H
pdate Client SSL Template						
		Gener	al Fields			
Name *	OOS-HLB-CSSL					
Auth Username	Common-name subject-alt-name subject-alt-name					
CA Certs					+ Add	
	Name	Clien	t OCSP Server	Client OCSP Service Group	Action	
Chain Certificate	OOSCert				( <b>*</b> )	
Server Certificate	OOSCert				•]	
Server Private Key	OOSCert				•	
Server Private Key Password Phrase						
Server Name List					+ Add	
	Name	Cert	Private Key	Password	Action	

Figure 36: Client SSL template configuration for Office Online Server

## **Cookie Persistence Configuration**

This section describes how to configure Cookie Persistence, which is used for Office Online Servers.

- 1. Go to ADC > Templates > Persistence.
- 2. Click Create > Persist Cookie to create a new Cookie Persistence template. In this test environment, the following data was used:
  - Name: PERSISTENCE-00S
- 3. Click OK after the configuration is completed, and then click Save to save the configuration.

Personal La Comun		v Thunder 4.1.
matines to Paralemente		Q He
Update Persist Cookie Templa	te	
Name *	PERSISTENCE/COS	
Expiration (seconds)		
Cookie Name	sto-id	
Domain		
Path	1	
Pass-thru mode	0	
Match Type		*
Insert Always	8	
Dont Honor Conn Rules	0	
Enable HttpOnly attribute	0	
Enable secure attribute	0	

Figure 37: Cookie Persistence template for Office Online Servers

# **Reverse Proxy**

This section describes how to configure Reverse Proxy for Skype for Business Server 2015 and OOS. Reverse Proxy is used for publishing Web Services of Skype Front End Server and Office Online Servers to remote access users through the Internet.

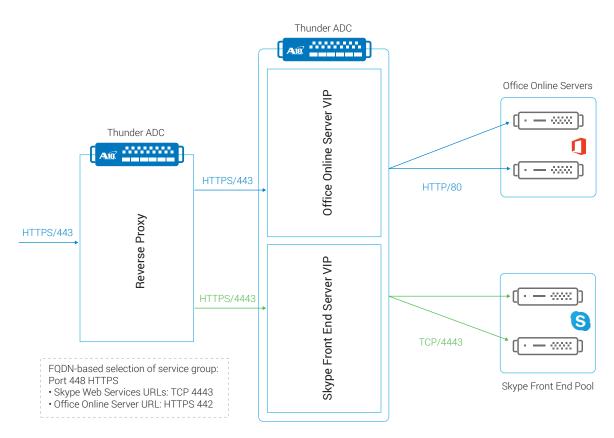


Figure 38: Load-balancing diagram for Reverse Proxy

## **Importing Certificate**

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

The Reverse Proxy uses TLS to communicate with the Front End ADC and thus you need to also import the root certificate of the CA, which issues the internal SSL server certificate for Skype Front End Pool and OOS. Usually, the internal enterprise CA is used for issuing internal SSL server certificates.

- 1. Go to ADC > SSL Management > SSL Certificates.
- 2. Click Import.
- 3. Import the root certificate issued by an internal enterprise CA. In this test environment, the following data is being used:
  - File Name: InternalRootCA
  - · Import: Certificate
  - Import Certificate from: Local
  - SSL or CA Certificate: CA Certificate
  - Certificate Format: DER (choose proper certificate file format)
  - · Certificate Source: Actual root certificate filename
- 4. Import the SSL certificate for remote user access. In this test environment, the certificate file contains published FQDN of both Skype Server 2015 Front End Pool and Office Online Servers:
  - File Name: SSL\_Cert
  - · Import: Certificate
  - Import Certificate from: Local
  - SSL or CA Certificate: SSL Certificate
  - Certificate Format: PEM (choose proper certificate file format)
  - Certificate Source: Actual SSL server certificate filename
- 5. If the private key for the SSL certificate is not stored with the certificate, import the SSL private key:
  - File Name: SSL\_Key
  - Import: Key
  - Import Key from: Local
  - Private Key Source: Actual SSL key filename

#### **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 Skype Front End Server and Office Online Server.

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

- 1. Go to ADC > Templates > SSL.
- Click Create > Client SSL to create a client SSL template. In this test environment, the following data is being used:
  - Name: CSSL1
  - Server Certificate: SSL\_Cert
  - Server Private Key: SSL\_Key
  - Server Private Key Password Phrase: Password for secret key
- 3. Click OK after the configuration is completed, and click Save to save the configuration.

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

parates Persitence 14 Press 13					1	munder 4.1.1-
						<b>O</b> Help
Update Client SSL Template						
		Genera	I Fields			•
Name *	CSSL1					
Auth Username	Common-name					
	B subject-alt-nam	ne-email				
	🗎 subject-alt-nam	ne-othername				
CA Certs					+ Add	
	Name	Client	OCSP Server	Client OCSP Service Group	Action	
Chain Certificate					+	
Server Certificate	SSICert				•	
Server Private Key	SSL_Key				•	
Server Private Key Password Phrase Server Name List					+ Add	

Figure 39: Client SSL template configuration for Reverse Proxy

Next create a Server SSL template with the following procedure:

- 1. Go to ADC > Templates > SSL.
- Click Create > Server SSL to create a server SSL template. In this test environment, the following data is being used:
  - Name: RP-Server-SSL
  - CA Certs: InternalRootCA

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

releation Persiatence 1.4 Protocols	s L7Prataciós SSL General			s Thunder 4.1
				• Hel
Update Server SSL Templa	ite			
Name *	RP-Server-SSL			
reactor	Contraction and the second			
CA Certs				+ Add
	Name	OCSP Server	Service Group	+ Add Action
		OCSP Server	Service Group	
	Name	OCSP Server	Service Group	Action

Figure 40: Server SSL template configuration for Reverse Proxy

#### **Server Configuration**

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

- 1. Go to ADC > SLB > Servers.
- 2. Click Create to create a new server. In this test environment, the following data is being used:
  - Name: Skype-Internal-VIP
  - Host: 10.0.3.123
  - Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)
- 3. Click on **Create** in the Port section:
  - Port Number: 4443
  - Protocol: TCP

- 4. Click Create.
- 5. Click Update after the configuration is done, and then click Save to save the configuration.
- 6. Repeat the above steps (from 2 to 5) to add an additional Office Online Server. In this test environment, the following data is being used:
  - Name: OOS-Internal-VIP
  - Host: 10.0.3.125
  - Health Monitor: Leave blank (Health Monitor is configured at the Service Group level)
  - Port Number: 443
  - Protocol: TCP

rtual	Servers	Virtual Services Services	vice Groups	Serv	ers Polic	y Limbs	Class Lists +	Applicati	ion G	lobal	Session -	- Resource	e Usage			vThunder	4.1.1-P1 buil
c	>> SLB	>> Servers															<b>⊖</b> He
N	ame 🗸	Search		bgs A	6	• Sea	rch Reset				C	Refresh	× Clear	Enable	O Disable	Telete	+ Create
	Status	Name	e Taos IP Address Health Monito		Ith Monitor	Connections Requests					By	rtes	ics Details	Actions			
-	Status	Name	Tags	112.1	address.	riea	itte Monitor	Current	Total	Peak	Total	Success	Forward	Receive	Statist	ics Details	Actions
白	0	OOS-Internal-VIP		10.0.3.	25 🖂	Default		0	134	0	0		0 183ME	8 83MB	Stat	s Charts	Edit
	0	tcp		443				0	134	0	0		0 183ME	83MB	11 (d	Stats	
1	0	Skype-internal-VIP		10.0.3	23 🗎	Defaul		0	437	0	0		0 2ME	8 16ME	Stat	s Charts	Edit
	0	tcp		4443				0	437	0	0		2 2ME	18MB	10	Stats	

Figure 41: Server list for Reverse Proxy

# **Service Group Configuration**

Configure Service Groups for Skype service.

- 1. Go to ADC > SLB > Service Groups.
- 2. Click **Create** to create a new Service Group for Skype service. In this test environment, the following data is being used:
  - Name: Skype-4443
  - Type: TCP
  - Algorithm: Least Connection
  - Health Monitor: HM
  - Member: Skype-Internal-VIP
  - Port: 4443
- 3. Click OK after the configuration is complete, and then click Save to save the configuration.
- 4. Repeat the above steps to configure a Service Group for OOS. In this test environment, the following data is being used:
  - Name: 00S-443
  - Type: TCP
  - · Algorithm: Least Connection
  - Health Monitor: HM
  - Member: OOS-Internal-VIP
  - Port: 443
- 5. Click OK after the configuration is completed, and then click Save to save the configuration.

A	10	Dashboard - Al	)C -	GSLE	- S	scurity + AAM +	CGN -	Netwo	k - S	ystem <del>-</del>							🗑 Partition	n: shared	~ 0	- • •	着 admin 🕞
ótusi	Servers	Virtual Services	Ser	vice Gro	ups	Servers Policy L	units (	Class Li	sts =	Applica	tion Glob	l Se	ision +	Resour	ce Us	age			v	Thunder 4	.1.1-P1 build 3
DC	> SLB	>> Service Group	5																		O Help
Ň	ame •	Search			Tags	Al	Search	R	eset								C Refresh	× Clea		Delete	+ Create
	Status	Name Tag		Tags	Туре	Algorithm		Con	nection	5	Reque	sts	By	tes			Servers		C1.0	tistics	Actions
	Status	reame		រងប្អូន	type	Aigonunii	Ci	arrent	Total	Peak	Success	Total	in l	Out	Up	Down	Disabled	Total	518	usues	Actions
8	0	OOS-443	8		tcp	Least Connection	<u>1</u>	0	134	0	0	Ð	83MB	183MB	1	0	(	1	Stats	Charts	Edit
	0	OOS-Internal-VIP		443				0	134	0	0	0	83MB	183MB					5	itats.	
	0	Skype-4443	8		tcp	Least Connection	0.5	0	437	0	0	Ð	18MB	2MB	1	0	(	1 1	Stats	Charts	Edit
	0	Skype-Internai-VIP		4443				0	437	0	0	0	18MB	2MB					15	State	

Figure 42: Service Group list for Reverse Proxy

# **Virtual Server Configuration**

Configure a virtual server for Skype and Office Online Services.

- 1. Go to ADC > SLB > Virtual Server.
- 2. Click Create to create a virtual server. In this test environment, the following data is being used:
  - Name: RP\_VIP
  - IP Address: 192.0.3.108
- 3. Go to the Virtual Port section and click Create to configure a virtual server port.
- 4. Fill in the Virtual Server Port setting section. In this test environment, the following data is being used:
  - Protocol: HTTPS
  - Port: 443
  - Service Group: Skype-4443
- 5. Expand the section General Fields:
  - Source NAT Auto: Enabled
  - aFleX Scripts: Skype-OOS-Selection (detail is provided in the aFlex Configuration section below)
- 6. Expand the section Templates:
  - Template Client SSL: CSSL1
  - Template Server SSL: RP-Server-SSL
- 7. Click Update after the configuration is done, and then click Save.

**NOTE**: To use the same VIP for published Skype Server 2015 and Office Online Servers, FQDN- and URL- based traffic distribution has to be configured and an aFleX script is also used in this test environment. The same thing can be carried out with the App Switching feature under the HTTP template.

tual S	lervers	Virtual Services S	ervice Groups	Servers	Policy Limits Class	s Lists + Apple	cation Glob	al Session	+ Resourc	e Usage		vThunder	4.1.1-P1 build
2 >	> SLB	>> Virtual Servers											<b>O</b> Hel
	ne •	Search	Tags	All	* Search	Reset		CRefres	× Clear	O Enable	O Disab	le 🗍 Delete	+ Create
Nar	ne •	Search			ocuren	reset		- Relies	Gear	C. Friddama	Cristal	a second	T Greate
Nar						<u></u> )	ections	1.310.00	Requests	Byt			
Nar	Statu		ime	Tags		<u></u> )	ections Total Pe			Byt		Statistics	Actions
Nar			ame			Conr			Requests	Byt	out		

Figure 43: Reverse Proxy virtual server

## aFleX Scripting 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. Go to ADC > aFleX.
- Click Create. In this test environment, the following script is configured to ensure that client access to Skype URLs such as lyncdiscover, meet, dialin, and sfbextweb are routed to the Skype-4443 service group, and client access to Office Online URL oos.<domain-name> is routed to OOS-443.

Name: Skype-OOS-Selection

```
Definition: Set info below:
```

```
when HTTP_REQUEST {
   set FQDN [string tolower [HTTP::host]]
   switch $FQDN {
        sfbextweb.al0test.com {pool Skype-4443}
   dialin.al0test.com {pool Skype-4443}
   meet.al0test.com {pool Skype-4443}
   lyncdiscover.al0test.com {pool Skype-4443}
   oos.al0test.com { pool OOS-443}
   }
}
```

NOTE: URL-based routing as shown above reduces the number of required public (external) IP addresses.

# Additional Security Feature – DDoS Mitigation (Optional)

The following section shows an additional security feature called DDoS Mitigation that can be implemented within the deployed solution.

### **DDoS Mitigation**

This section describes an additional security feature to protect applications from Distributed Denial of Service (DDoS) attacks. To configure this feature within the ACOS solution, navigate to Security > > DDoS.

The DDoS protection feature is a global configuration. To enable this feature, select the necessary DDoS attacks you would like to drop. In Figure 44, we have selected the DDoS attack mitigation required. Once completed, click Update and Save to save the configuration.

Dashboard - ADC	GSLB • Security • AAM • CGN • Network • System •	📽 Partition: shared 🗸 🥥 🗸 🔀 🚔 admin 🕞
s		vThunder 4.1.1-P1 build (
rrity >> DDoS Protection		9 Help
pdate DDoS Protection		
IP Anomaly Drop	Drop All	
	🗷 Frag	
	IP Option	
	😢 Land Attack	
	R Packet Deformity Layer 3	
	Packet Deformity Layer 4	
	Ping of Death	
	Security Attack Layer 3	
	Security Attack Layer 4	
	CP No Flag	
	TCP Syn Fin	
	TCP Syn Frag	
Bad Content	10	
Out of Sequence	10	
Zero Window	10	
ICMP Rate Limiting Rate		

#### Figure 44: DDoS protection

The following IP anomaly filters are supported for system-wide Policy-Based Server Load Balancing (PBSLB), although you can also use them with¬out PBSLB:

- Invalid HTTP or SSL payload
- Zero-length TCP window
- Out-of-sequence packet

NOTE: These filters are supported only for HTTP and HTTPS traffic.

# **Summary**

This document describes how to configure Thunder ADC as a Reverse Proxy to support Microsoft Skype for Business Server 2015 and Office Online Server.

Deploying Thunder ADC as a load balancer and Reverse Proxy for Microsoft Skype for Business Server 2015 and OOS offers the following features and benefits:

- Transparent application load sharing
- · High availability for Skype servers, ensuring users can access Skype applications without disruption
- Scalability, as the Thunder ADC device transparently load balances multiple Skype communication servers
- · Higher connection throughput to enhance end user experience
- · Improved server performance due to server offloading, including SSL Offload
- · Protection against DDoS attacks using integrated DDoS protection capabilities
- · Protection against web application attacks through Web Application Firewall (WAF)
- · Consolidated roles on a single platform through multiple partitions

Thunder ADC offers a cost-effective way for organizations to optimize their Skype for Business Server 2015 deployments, empowering employees to connect, communicate, and collaborate with Skype.

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

https://www.a10networks.com/products/thunder-series/thunder-application\_delivery\_controller

https://www.a10networks.com/resources/solution-briefs

https://www.a10networks.com/resources/case-studies

# Appendix

Here is the Thunder ADC configuration used in an actual test environment.

## Skype Server 2015 Front End

```
vlan 103
 untagged ethernet 2
 router-interface ve 103
!
vlan 104
 untagged ethernet 3
 router-interface ve 104
!
vlan 105
 untagged ethernet 4
 router-interface ve 105
!
hostname Internal_FE
1
interface management
 ip address 10.100.2.130 255.255.255.0
 ip default-gateway 10.100.2.1
!
interface ethernet 1
1
interface ethernet 2
 enable
!
interface ethernet 3
 enable
1
interface ethernet 4
 enable
I.
interface ve 103
 ip address 10.0.3.1 255.255.255.0
!
interface ve 104
 ip address 10.0.2.1 255.255.255.0
!
interface ve 105
 ip address 10.0.5.1 255.255.255.0
!
T
ip route 0.0.0.0 /0 10.0.5.254
!
health monitor HM
!
health monitor OOS-80
 interval 30 timeout 10
 method http port 80 expect wopi-discovery url GET /hosting/discovery
!
slb template persist cookie PERSISTENCE-OOS
!
```

```
slb template persist source-ip SIP
 timeout 20
T
slb template tcp TCP
 idle-timeout 1800
!
slb server FE1 10.0.3.12
 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
!
slb server FE2 10.0.3.13
 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
L
slb server 00S1 10.0.3.15
 port 80 tcp
!
slb server 00S2 10.0.3.16
 port 80 tcp
!
slb service-group 135 tcp
 method least-connection
 health-check HM
 member FE1 135
 member FE2 135
!
slb service-group 443 tcp
 method least-connection
 health-check HM
 member FE1 443
 member FE2 443
!
slb service-group 444 tcp
 method least-connection
 health-check HM
 member FE1 444
```

```
member FE2 444
!
slb service-group 4443 tcp
 method least-connection
 health-check HM
 member FE1 4443
 member FE2 4443
!
slb service-group 5061 tcp
 method least-connection
 health-check HM
 member FE1 5061
 member FE2 5061
T
slb service-group 5065 tcp
 method least-connection
 health-check HM
 member FE1 5065
 member FE2 5065
!
slb service-group 5070 tcp
 method least-connection
 health-check HM
 member FE1 5070
 member FE2 5070
!
slb service-group 5071 tcp
 method least-connection
 health-check HM
 member FE1 5071
 member FE2 5071
!
slb service-group 5072 tcp
 method least-connection
 health-check HM
 member FE1 5072
 member FE2 5072
!
slb service-group 5073 tcp
 method least-connection
 health-check HM
 member FE1 5073
 member FE2 5073
!
slb service-group 5075 tcp
 method least-connection
 health-check HM
 member FE1 5075
 member FE2 5075
!
slb service-group 5076 tcp
 method least-connection
 health-check HM
 member FE1 5076
 member FE2 5076
!
```

```
slb service-group OOS-SG-80 tcp
 method least-connection
 health-check OOS-80
 member OOS1 80
 member OOS2 80
!
slb template client-ssl OOS-HLB-CSSL
 chain-cert OOSCert
 cert OOSCert
 key OOSCert pass-phrase encrypted
qVNqrbV6DCe3hBv+jr0G4zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
1
slb virtual-server FEVIP 10.0.3.123
 port 135 tcp
   name 10.0.3.123 TCP 135
   source-nat auto
   service-group 135
   template persist source-ip SIP
    template tcp TCP
 port 443 tcp
   name 10.0.3.123 TCP 443
   source-nat auto
   service-group 443
   template persist source-ip SIP
   template tcp TCP
 port 444 tcp
   name 10.0.3.123 TCP 444
   source-nat auto
    service-group 444
   template persist source-ip SIP
   template tcp TCP
 port 4443 tcp
   name 10.0.3.123 TCP 4443
   source-nat auto
   service-group 4443
   template persist source-ip SIP
    template tcp TCP
 port 5061 tcp
   name 10.0.3.123 TCP 5061
    source-nat auto
   service-group 5061
   template persist source-ip SIP
   template tcp TCP
 port 5065 tcp
   name 10.0.3.123 TCP 5065
   source-nat auto
    service-group 5065
   template persist source-ip SIP
   template tcp TCP
 port 5070 tcp
   name 10.0.3.123 TCP 5070
   source-nat auto
   service-group 5070
   template persist source-ip SIP
    template tcp TCP
 port 5071 tcp
```

```
name 10.0.3.123 TCP 5071
    source-nat auto
    service-group 5071
    template persist source-ip SIP
    template tcp TCP
 port 5072 tcp
   name 10.0.3.123 TCP 5072
   source-nat auto
   service-group 5072
   template persist source-ip SIP
    template tcp TCP
 port 5073 tcp
   name 10.0.3.123 TCP 5073
    source-nat auto
    service-group 5073
   template persist source-ip SIP
   template tcp TCP
 port 5075 tcp
   name _10.0.3.123_TCP_5075
   source-nat auto
   service-group 5075
   template persist source-ip SIP
   template tcp TCP
 port 5076 tcp
   name _10.0.3.123_TCP_5076
    source-nat auto
   service-group 5076
   template persist source-ip SIP
    template tcp TCP
I.
slb virtual-server OOS-VIP 10.0.3.125
 port 443 https
   name OOS-VIP 443 https
   source-nat auto
   service-group OOS-SG-80
   template persist cookie PERSISTENCE-OOS
    template client-ssl OOS-HLB-CSSL
!
end
```

#### Skype Server 2015 Internal Edge

```
vlan 106
    untagged ethernet 3
    router-interface ve 106
!
vlan 401
    untagged ethernet 2
    router-interface ve 401
!
hostname Internal_Edge
!
interface management
```

```
ip address 10.100.2.136 255.255.255.0
 ip default-gateway 10.100.2.1
 enable
!
interface ethernet 1
!
interface ethernet 2
 enable
!
interface ethernet 3
 enable
1
interface ve 106
 ip address 10.0.6.241 255.255.255.0
!
interface ve 401
 ip address 10.0.4.241 255.255.255.0
I.
!
ip route 0.0.0.0 /0 10.0.6.254
!
health monitor HM
!
slb template persist source-ip SIP
T
slb template tcp TCP
 idle-timeout 1800
!
slb server InternalEdge-1 10.0.4.31
 port 443 tcp
 port 3478 udp
 port 5061 tcp
 port 5062 tcp
T
slb server InternalEdge-2 10.0.4.32
 port 443 tcp
 port 3478 udp
 port 5061 tcp
 port 5062 tcp
T
slb service-group InternalEdge-3478 udp
 method least-connection
 health-check HM
 member InternalEdge-1 3478
 member InternalEdge-2 3478
!
slb service-group InternalEdge-443 tcp
 method least-connection
 health-check HM
 member InternalEdge-1 443
 member InternalEdge-2 443
!
slb service-group InternalEdge-5061 tcp
 method least-connection
 health-check HM
 member InternalEdge-1 5061
```

```
member InternalEdge-2 5061
!
slb service-group InternalEdge-5062 tcp
 method least-connection
 health-check HM
 member InternalEdge-1 5062
 member InternalEdge-2 5062
!
slb virtual-server IEVIP 10.0.4.30
 port 443 tcp
   name Internal-443
   source-nat auto
   service-group InternalEdge-443
   template persist source-ip SIP
    template tcp TCP
 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 persist source-ip SIP
    template tcp TCP
 port 5062 tcp
   name Internal-5062
    source-nat auto
    service-group InternalEdge-5062
   template persist source-ip SIP
    template tcp TCP
!
end
```

### Skype Server 2015 External Edge

```
vlan 102
 untagged ethernet 2
  router-interface ve 102
1
vlan 110
 untagged ethernet 3
  router-interface ve 110
!
hostname External Edge
!
interface management
  ip address 10.100.2.132 255.255.255.0
  ip default-gateway 10.100.2.1
  enable
I.
interface ethernet 1
```

I.

```
interface ethernet 2
 enable
!
interface ethernet 3
 enable
I.
interface ve 102
 ip address 192.0.2.1 255.255.255.0
!
interface ve 110
 ip address 192.0.3.1 255.255.255.0
!
L
ip route 0.0.0.0 /0 192.0.3.254
!
health monitor HM
!
slb template persist source-ip SIP
!
slb template tcp TCP
 idle-timeout 1800
1
slb server ExternalEdge1-access 192.0.2.21
 port 443 tcp
 port 5061 tcp
1
slb server ExternalEdge1-av 192.0.2.23
 port 443 tcp
 port 3478 udp
1
slb server ExternalEdge1-web 192.0.2.22
 port 443 tcp
 port 3478 udp
!
slb server ExternalEdge2-access 192.0.2.31
 port 443 tcp
 port 5061 tcp
!
slb server ExternalEdge2-av 192.0.2.33
 port 443 tcp
 port 3478 udp
!
slb server ExternalEdge2-web 192.0.2.32
 port 443 tcp
 port 3478 udp
T
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
I
slb service-group ExternalEdge-av-3478 udp
 method least-connection
 health-check HM
 member ExternalEdge1-av 3478
 member ExternalEdge2-av 3478
!
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-web-443 tcp
 method least-connection
 health-check HM
 member ExternalEdge1-web 443
 member ExternalEdge2-web 443
I.
slb virtual-server _192.0.2.111_vserver 192.0.2.111
 port 443 tcp
   name ExternalEdge-ac443
    service-group ExternalEdge-access-443
    template persist source-ip SIP
    template tcp TCP
!
slb virtual-server 192.0.2.112 vserver 192.0.2.112
 port 443 tcp
   name ExternalEdge-web443
    service-group ExternalEdge-web-443
    template persist source-ip SIP
    template tcp TCP
!
slb virtual-server 192.0.2.113 vserver 192.0.2.113
 port 443 tcp
   name ExternalEdge-av443
   service-group ExternalEdge-av-443
   template persist source-ip SIP
    template tcp TCP
 port 3478 udp
   name ExternalEdge-av3478
    service-group ExternalEdge-av-3478
    template persist source-ip SIP
ļ
```

```
end
```

#### **Reverse Proxy**

```
ip anomaly-drop packet-deformity layer-3
ip anomaly-drop packet-deformity layer-4
ip anomaly-drop security-attack layer-3
ip anomaly-drop security-attack layer-4
```

```
ip anomaly-drop bad-content 10
ip anomaly-drop frag
ip anomaly-drop ip-option
ip anomaly-drop land-attack
ip anomaly-drop out-of-sequence 10
ip anomaly-drop ping-of-death
ip anomaly-drop tcp-no-flag
ip anomaly-drop tcp-syn-fin
ip anomaly-drop tcp-syn-frag
ip anomaly-drop zero-window 10
!
vlan 106
 untagged ethernet 3
 router-interface ve 106
1
vlan 110
 untagged ethernet 2
  router-interface ve 110
!
hostname ReverseProxy
!
interface management
 ip address 10.100.2.134 255.255.255.0
  ip default-gateway 10.100.2.1
  enable
!
interface ethernet 1
1
interface ethernet 2
 enable
!
interface ethernet 3
  enable
1
interface ve 106
  ip address 10.0.6.201 255.255.255.0
!
interface ve 110
  ip address 192.0.3.201 255.255.255.0
T
!
ip route 0.0.0.0 /0 192.0.3.254
1
ip route 10.0.2.0 /24 10.0.6.254
1
ip route 10.0.3.0 /24 10.0.6.254
!
ip route 10.0.5.0 /24 10.0.6.254
1
health monitor HM
!
slb template persist source-ip RP
!
slb template server-ssl RP-Server-SSL
  ca-cert InternalRootCA
!
```

```
slb server OOS-Internal-VIP 10.0.3.125
 port 443 tcp
I
slb server Skype-Internal-VIP 10.0.3.123
 port 4443 tcp
ļ
slb service-group OOS-443 tcp
 method least-connection
 health-check HM
 member OOS-Internal-VIP 443
!
slb service-group Skype-4443 tcp
 method least-connection
 health-check HM
 member Skype-Internal-VIP 4443
!
slb template client-ssl CSSL1
 cert SSL Cert
  key SSL Key pass-phrase encrypted
yKfJxqqqJak8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb virtual-server RP VIP 192.0.3.108
 port 443 https
    aflex Skype-OOS-Selection
    source-nat auto
    service-group Skype-4443
    template server-ssl RP-Server-SSL
    template client-ssl CSSL1
I
end
```

## 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**

#### Worldwide Offices

North America

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-16163-EN-01

May 2017

sales@a10networks.com Europe emea\_sales@a10networks.com South America

latam\_sales@a10networks.com Japan jinfo@a10networks.com China

Hong Kong hongkong@a10networks.com Taiwan taiwan@a10networks.com Korea korea@a10networks.com South Asia southasia@a10networks.com Australia/New Zealand china\_sales@a10networks.com anz\_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at a10networks.com/contact or call to speak with an A10 sales representative.

©2017 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, A10 Harmony, A10 Lightning, ACOS, Thunder and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.