Deploying Skype for Business Server 2015 with NetScaler

Deployment Guide

This guide focuses on defining the deployment process for Microsoft Skype for Business with Citrix NetScaler

Table of Contents

Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications. It provides availability, scalability, optimization and security for Microsoft Skype for Business deployments.

Citrix is strongly committed to its partnership with Microsoft. For several years, Citrix has completed certifications and provided deployment guides for key Microsoft applications including Lync, Exchange, SharePoint and Dynamics CRM. NetScaler's rich application delivery capabilities significantly enhance the performance of these enterprise applications.

This guide defines the process for deploying Microsoft Skype for Business Server 2015 with NetScaler. Microsoft Skype for Business Server 2015 is an enterprise collaboration, messaging and telephony platform and is the successor to Lync 2013.

Overview of Microsoft Skype for Business

Skype for Business Server Roles

- There are two server topologies that can be used for Skype for Business. The Standard Editiontopology is designed for small organizations, and pilot projects in large organizations. It enables many Skype for Business Server features such as instant messaging (IM), presence, confer- encing, and Enterprise Voice, including the necessary databases to run on a single server. This enables Skype for Business Server functionality at a lower cost, but does not provide a truly highly available solution.
- Enterprise Edition topologies allow features such as pooling of servers with multiple roles; which allow for high availability.
- The primary difference between these editions is support for high-availability features that are only included in the Enterprise Edition. To implement high-availability, multiple Front-End servers must be deployed to a pool and SQL Servers need to be mirrored. Standard Edition servers cannot be pooled.
- An Enterprise Edition deployment enables the creation of multiple servers with different roles.

The primary roles are –

- Front end servers
- Edge servers
- Director servers
- Database (SQL) servers

Front End Servers

The front end server runs most basic functions, and plays a critical role in the deployment. This server role must be deployed in an Enterprise Edition deployment, in addition to the Database server that hosts the SQL Server instance that holds the Skype for Business database.

A front end pool includes identically configured front end servers that work together to provide services for a common group of users. This type of configuration provides improved scalability and failover.

The front end server performs the following functions:

- User authentication and registration
- Presence information and contact card exchange
- Address book services and distribution list expansion
- IM functionality, including multi-party IM conferences
- Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed)
- Application hosting for applications included with Skype for Business Server (for example, Conferencing Attendant and Response Group application) and third-party applications
- Option: monitoring-collection of usage information in the form of call detail records (CDRs) and call error records (CERs). This information provides metrics about the quality of the media (audio and video) traversing the network for both Enterprise voice calls and A/V conferences.
- Web components of supported web-based tasks such as Web Scheduler and Join Launcher.
- Optional: Archiving - archival of IM communications and meeting content for compliance.
- Optional: Persistent Chat Web Services for Chat Room management and Persistent Chat Web Services for File Upload/Download [if persistent chat is enabled]
- Front end pools are the primary store for user and conference data. Information about each user is replicated amongst the servers in the pool, and backed up on the database servers.
- Additionally, one front end server in the deployment serves as the Central Management Server, which manages and deploys basic configuration data to all servers running Skype for Business services. The central management server also provides server management shell and file trans- fer capabilities for Skype for Business. During the implementation, management tools such as the Skype for Business topology builder should be installed on this server.
- The database servers run Microsoft SQL Server and provide the database services for the front end pool. They serve as backup stores for user and conference data, and are the primary stores for other databases such as the response group database. A deployment with a single data- base server is possible but a solution that uses SQL Server mirroring is recommended for failover. Skype for Business is not installed on database servers.

Edge Servers

- Edge servers enable users to communicate with external users outside of the organization's core network. These users might include employees working offsite, business partners, and users that were invited to join hosted Skype for Business meeting conferences. The edge server is also responsible for enabling connectivity to public IM services, such as Windows Live, Skype, and Google Talk.
- Edge servers enable mobile support for Skype for Business. Users on supported mobile devices (Apple iOS, Android, Windows Phone or Nokia) can perform activities such as sending and receiving instant messages, viewing contacts, and viewing presence. In addition, some enter- prise voice features, such as click to join a conference, call via work, single number reach, voice mail, and missed calls are also supported. Push notifications are supported for mobile devices that don't support applications running in the background.
- Edge servers include a fully-integrated Extensible Messaging and Presence Protocol (XMPP) proxy, with an XMPP gateway included on front end servers. Configuring the XMPP compo- nents enables Skype for Business Server 2015 users to add contacts from XMPP-based partners (such as Google Talk) for instant messaging and presence.

Mediation Server

- The Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. It translates signalling, and, in some configurations, media. It can mediate traffic between your internal Skype for Business server and public switched telephone network (PSTN) gateways, IP-PBX, or a Session Initiation Protocol (SIP) trunk. The mediation server can be located on the same server as the front end server, or separated in a stand-alone mediation server pool.

Director Servers

- Director servers can authenticate Skype for Business user requests but they do not store user account information, provide presence, or conferencing services. They are most useful for enhanced security in deployments that require external user access. The director servers authenticate requests before sending them to internal servers. In the event of a denial-of-ser- vice attack, the attack ends with the Director and does not reach the Front End Servers.

Persistent Chat Front End Servers

- Persistent chat enables users to participate in multiparty, topic-based conversations that persist over time. The persistent chat front end server runs this service, while the persistent chat database server stores the chat history data, and information about categories and chat rooms. The optional persistent chat compliance back end server can store chat content and events for compliance purposes.
- Deployments running Skype for Business Server Standard Edition can run persistent chat on the same server. You cannot configure a persistent chat front-end server and Enterprise Edition front- end server on the same server.

Workload Types

Instant Messaging and Presence

- Instant messaging (IM) enables users to communicate with each other in real time on their com- puters using text-based messages. Both two-party and multiparty IM sessions are supported. A participant in a two-party IM conversation can add a third participant to the conversation at any time. When this happens, the cConversation window changes to support conferencing features.

- Presence provides information to users about the status of other users on the network. A user's presence status provides information to help others decide whether they should try to contact the user and whether to use instant messaging, phone, or email. Presence encourages instant com- munication when possible, but it also provides information about whether a user is in a meeting or out of the office, indicating that instant communication is not possible. This presence status is dis- played as a presence icon in Skype for Business and other presence-aware applications, including Microsoft Outlook, SharePoint, Word, and Excel. The presence icon represents the user's current availability and willingness to communicate.

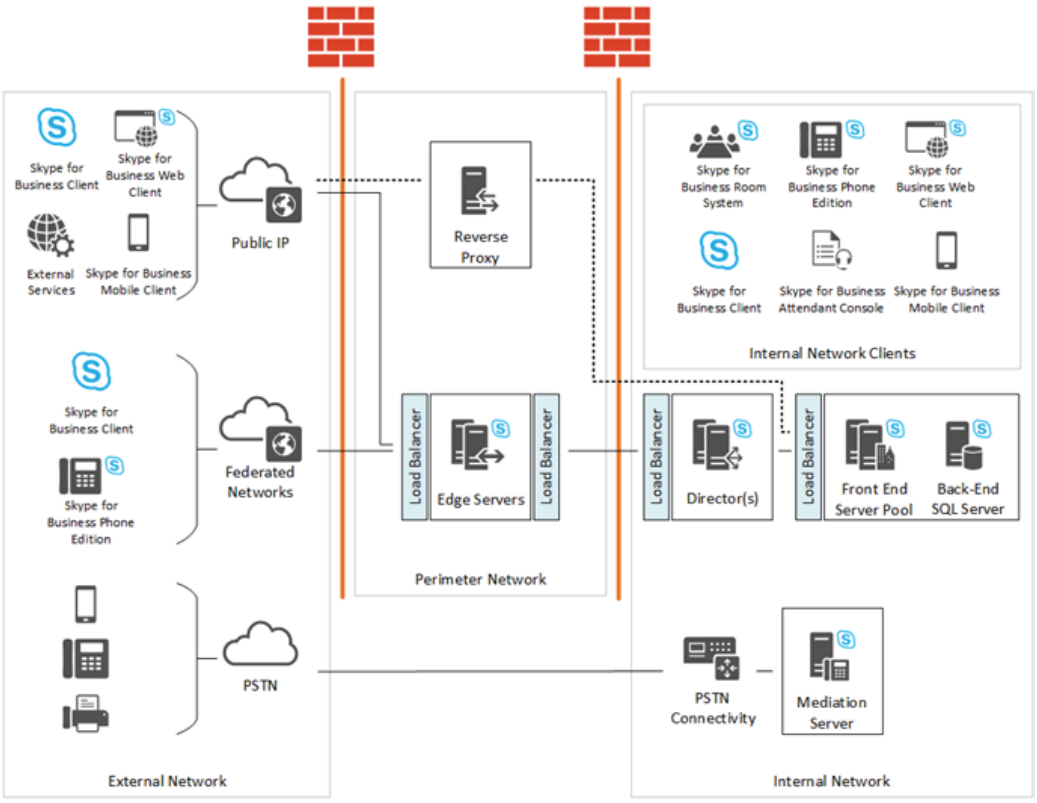
Audio/Video & Web Conferencing

- With web conferencing, users can share and collaborate on documentsduring meetings and conference sessions. Additionally, users can share all or part of their desktop with each other in real time.
- A/V conferencing enables real-time audio and video communications between users.

Enterprise Voice

- Skype for Business Server 2015 supports multiple trunks between mediation servers and gate- ways. A trunk is a logical association between a port number and mediation server with a port number and gateway. This means that a mediation server can have multiple trunks to different gateways, and a gateway can have multiple trunks to different mediation servers. Inter-trunk routing makes it possible for Skype for Business to interconnect an IP-PBX to a public switched telephone network (PSTN) gateway or to interconnect multiple IP-PBX systems.
- Skype for Business serves as the glue (that is, the interconnection) between different telephony systems. Microsoft Skype for Business Server 2015 makes improvements in the areas of call forwarding, simultaneous ringing, voice mail handling, and caller ID presentation.

Recommended topology for Hardware Load Balancers and Reverse Proxy



Front End Pool internal interface load balancer setting

The configuration mentioned in the later sections of this guide will need to be duplicated for all of the individual servers/services mentioned here.

Server	NetScaler VServer Port	Node Port/ Forward to	Port Type	NetScaler Persistence Profile	Description
Front End	443	443	TCP	Source IP	Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Front End	135	135	TCP	Source IP	RPC
Front End	444	444	TCP	Source IP	HTTPS – Intra and Interpool communication
Front End	5061	5061	TCP	Source IP	SIP/MTLS
Front End	443	4443	TCP	Source IP	HTTPS
Front End	80	8080	TCP	Source IP	HTTP
Front End	5065	5065	TCP	Source IP	Used for incoming SIP listening requests for application sharing.
Front End	5071	5071	TCP	Source IP	Used for incoming SIP requests for the Response Group application.
Front End	5072	5072	TCP	Source IP	Used for incoming SIP requests for Attendant (dial in conferencing).
Front End	5073	5073	TCP	Source IP	Used for incoming SIP requests for the Skype for Business Server Conferencing Announcement service (that is, for dial-in conferencing).
Front End	5075	5075	TCP	Source IP	Used for incoming SIP requests for the Call Park application.
Front End	5076	5076	TCP	Source IP	Used for incoming SIP requests for the Audio Test service.
Front End	5080	5080	TCP	Source IP	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.
Front End	448	448	TCP	Source IP	Used for call admission control by the Skype for Business Server Bandwidth Policy Service.

Front End Pool external interface load balancer setting

Server	NetScaler VServer Port	Node Port/ Forward to	Port Type	NetScaler Persistence Profile	Description
Front End	443	443	TCP	Source IP	Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Front End	443	4443	TCP	Source IP	RPC
Front End	80	8080	TCP	No Persistence	HTTPS – Intra and Interpool communication

Director Pool Load balancer settings

Server	NetScaler VServer Port	Node Port/ Forward to	Port Type	NetScaler Persistence Profile	Description
Director	443	443	TCP	None	Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Director	443	4443	TCP	None	HTTPS
Director	80	8080	TCP	None	HTTP
Director	5061	5061	TCP	None	Used for internal communications between servers and for client connections.

Edge internal interface load balancer setting

Server	NetScaler VServer Port	Node Port/ Forward to	Port Type	NetScaler Persistence Profile	Description
A/V	443	443	TCP	Source IP	Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Access	5061	5061	TCP	Source IP	Used for internal ports for SIP/MTLS communication for remote user access or federation.
A/V	5062	5062	TCP	Source IP	Used for internal ports for SIP/MTLS authentication of IM communications flowing outbound through the internal firewall. (MRAS authentication)
A/V	3478	3478	UDP	Source IP	Used for internal ports for STUN/ UDP inbound and outbound media communications.

Edge External Load Balancer Settings

Server	NetScaler VServer Port	Node Port/ Forward to	Port Type	NetScaler Persistence Profile	Description
A/V, Access, Web Conf	443	443	TCP	Source Address Affinity	Used for external ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
Access	5061	5061	TCP	Source Address Affinity	Used for external ports for SIP/MTLS communication for remote user access or federation.
A/V	3478	3478	UDP	Source Address Affinity	Used for external ports for STUN/ UDP inbound and outbound media communications.

Note: For the vi rtual servers that are created for the A/V Edge Ext ernal services (on port 443 and 3478 as described above), USIP mode (Use Source IP) should be enabled for the backend services. Also, the useproxyport setting on the virtual servers should be disabled. These settings can be found in the Basic settings screen for the virtual server and services.

Port information for Reverse Proxy External interface

Description	Port	Destination IP	Source IP
Address book downloads, Address Book Web Query service, Auto-Discover, client updates, meeting content, device updates, Group expansion, Office Web Apps for conferencing, dial-in conferencing, and meetings.	443	Reverse proxy listener (Virtual Server IP on NetScaler)	Any

Port information for Reverse Proxy Internal interface

Description	Port	Destination IP	Source IP
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.	4443	Front End Server, Front End pool, Director, Director pool	Internal reverse proxy interface

Load Balancing Microsoft Skype for Business 2015 with NetScaler

Recommended Topology for load balancinginternal traffic

For this scenario, NetScaler acts as the HLB for Skype for Business, load balancing various enter- prise server roles. To assist in understanding the required network setup, we will use the following convention –

- Network A: Internal Network (such as 192.168.1.x)
- Network B: External/Perimeter Network (such as 10.10.1.x) with Internet connectivity

Lab Setup

Role	FQDN	IP Network Interfaces	Additional Information
Active Directory	dc.yourdomain.com	192.168.1.x	Domain Controller & DNS
SQL Server 2014	sqlsfb.yourdomain.com	192.168.1.x	Default Instance for Skype for Business 2015
Skype for Business 2015 Front-End 1	sfbfe1.yourdomain.com	192.168.1.x	Pool Name: pool. yourdomain.com
Skype for Business 2015 Front-End 2	sfbfe2.yourdomain.com	192.168.1.x	Pool Name: pool. yourdomain.com
Skype for Business 2015 Director 1	sfbdir1.yourdomain.com	192.168.1.x	Pool Name: dirpool. yourdomain.com
Skype for Business 2015 Director 2	sfbdir2.yourdomain.com	192.168.1.x	Pool Name: dirpool. yourdomain.com
Outlook Web App server	owa.yourdomain.com	192.168.1.x	
NetScaler		10.10.1.x	
Front End Pool	pool.Yourdomain.com	192.168.1.61	NS VIP 1
Director Pool	dirpool.yourdomain.com	192.168.1.62	NS VIP 2
OWA Pool	owa.yourdomain.com	192.168.1.63	NS VIP 3

Configuring NetScaler for enabling Skype for Business internal traffic

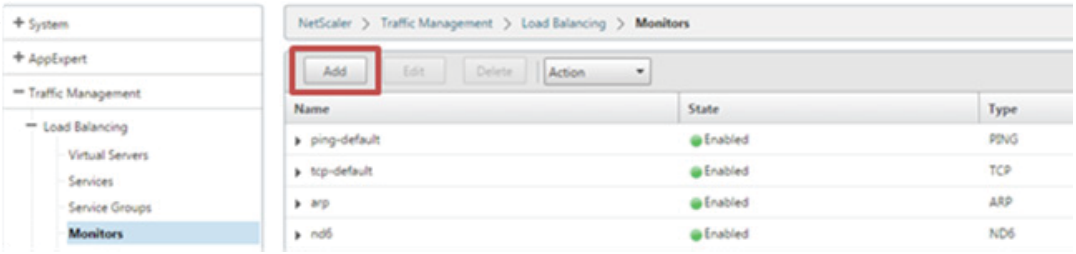
To enable Skype for Business usage over the internal network on a NetScaler load balanced envi- ronment, perform the following steps –

Note: Of the services listed in the tables earlier, you may choose to deploy some or all of the ser- vices in your Skype for Business deployment. Perform the steps mentioned below only for the Skype for Business services deployed in your environment; when services that are not deployed in your Skype for Business environment are provisioned on NetScaler, theywill be shown as Down.

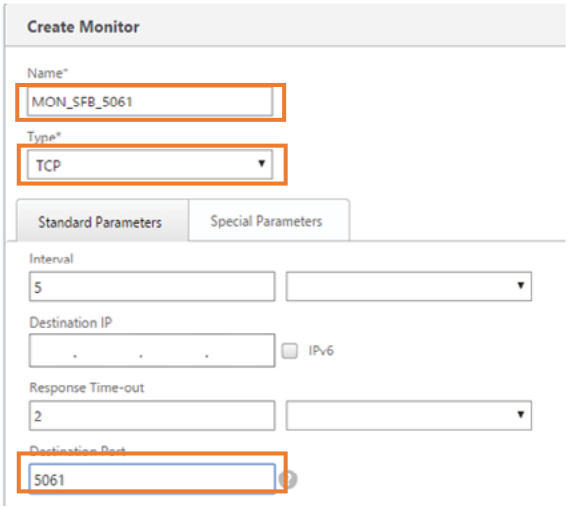
Step 1: Add Custom Monitors

Configure custom monitors for all applicable ports in the deployment. To determine the list of monitors to be configured, refer to the list of internal server ports listed in the Recommended Topology section presented earlier.

These monitors need to be enabled for each port to ensure that Skype for Business services are up and running. A generic monitor may determine that the server is up (since itresponds to ping requests) and continue to forward requests to servers, even though the actual Skype for Business service may be down.



Add an individual monitor for each service as shown below (the example port used is 5061)



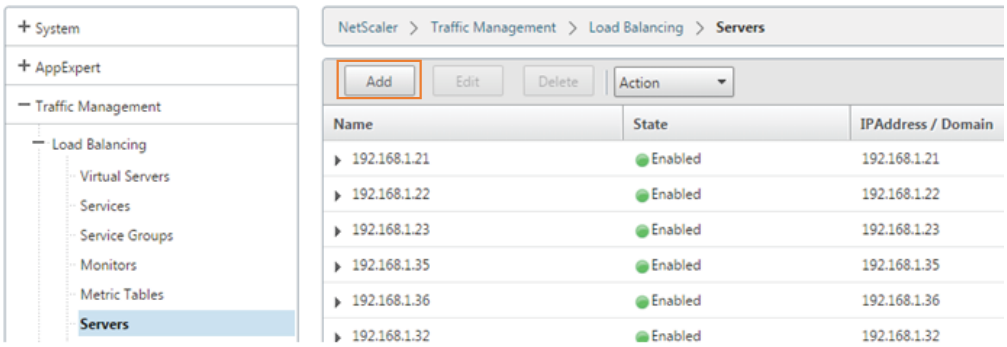
Use the following template for settings in the Create Monitor window for each monitor –

Setting	Value
Name	MON_SFB_<Port Number>
Type	TCP
Standard Parameters>Interval	5 Seconds
Standard Parameters> Response Time-out	2 Seconds
Standard Parameters> Destination Port	<Port Number>

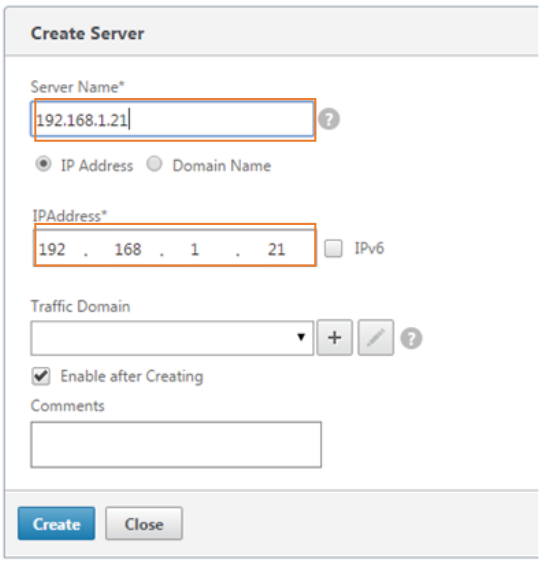
(Here, <Port Number> refers to the port number for the particular service that you are configuring the monitor for)

Step 2: Add Skype for Business application servers

Next, add the Skype for Business application servers to the NetScaler appliance by navigating to Traffic Management>Load Balancing>Servers and clicking the Add button, as shown below -



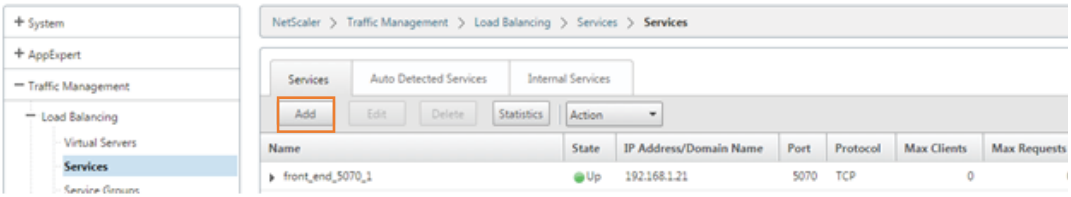
This will show the Create Server prompt, shown below. Provide a meaningful server name (or retain the IP address as shown below) and the IP Address of the server. All the servers that are being load balanced (Front End, Edge, Director or Database) should be added in this manner.



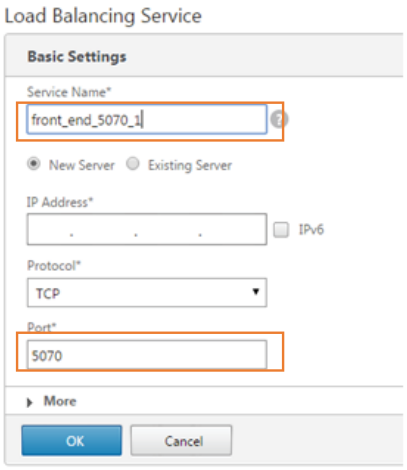
After adding the servers, verify that they are enabled by looking at the list of servers in the Servers list at Traffic Management>Load Balancing>Servers

Step 3: Create Skype for Business Services

Now, add services corresponding to the various Skype for Business services (listed in the tables pre- sented earlier) to the NetScaler appliance by navigating to Traffic Management>Load Balancing>Services and clicking the Add button, as shown below -

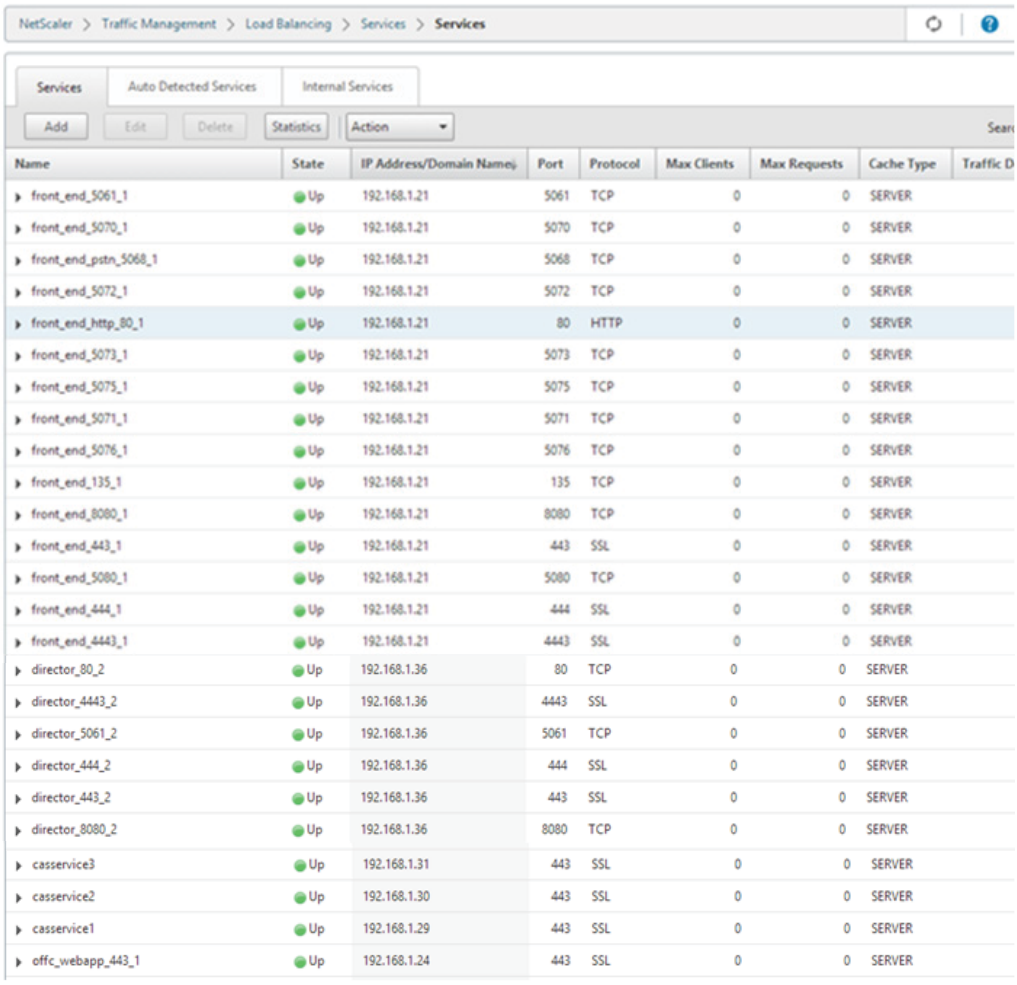


In the Load Balancing Service section, add an appropriate service name (as shown below) and port number as detailed in the tables for each of the services that are to be deployed over NetScaler.



After completing this configuration, click OK. Other additional features such as AppFlow logging can be enabled by clicking the More option, however this is not required for this configuration.

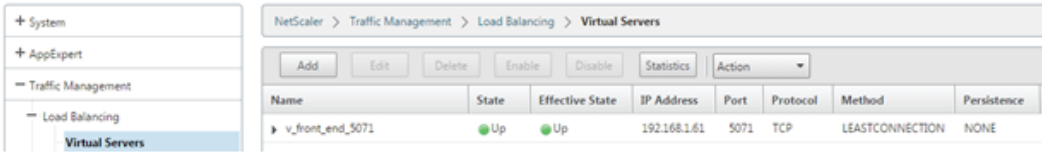
After completing the configuration as stated above, you should see the following list of services in your NetScaler device (or a subset, depending upon the services you have chosen to deploy).



Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic D
front_end_5061_1	Up	192.168.1.21	5061	TCP	0	0	SERVER	
front_end_5070_1	Up	192.168.1.21	5070	TCP	0	0	SERVER	
front_end_pstn_5068_1	Up	192.168.1.21	5068	TCP	0	0	SERVER	
front_end_5072_1	Up	192.168.1.21	5072	TCP	0	0	SERVER	
front_end_http_80_1	Up	192.168.1.21	80	HTTP	0	0	SERVER	
front_end_5073_1	Up	192.168.1.21	5073	TCP	0	0	SERVER	
front_end_5075_1	Up	192.168.1.21	5075	TCP	0	0	SERVER	
front_end_5071_1	Up	192.168.1.21	5071	TCP	0	0	SERVER	
front_end_5076_1	Up	192.168.1.21	5076	TCP	0	0	SERVER	
front_end_135_1	Up	192.168.1.21	135	TCP	0	0	SERVER	
front_end_8080_1	Up	192.168.1.21	8080	TCP	0	0	SERVER	
front_end_443_1	Up	192.168.1.21	443	SSL	0	0	SERVER	
front_end_5080_1	Up	192.168.1.21	5080	TCP	0	0	SERVER	
front_end_444_1	Up	192.168.1.21	444	SSL	0	0	SERVER	
front_end_4443_1	Up	192.168.1.21	4443	SSL	0	0	SERVER	
director_80_2	Up	192.168.1.36	80	TCP	0	0	SERVER	
director_4443_2	Up	192.168.1.36	4443	SSL	0	0	SERVER	
director_5061_2	Up	192.168.1.36	5061	TCP	0	0	SERVER	
director_444_2	Up	192.168.1.36	444	SSL	0	0	SERVER	
director_443_2	Up	192.168.1.36	443	SSL	0	0	SERVER	
director_8080_2	Up	192.168.1.36	8080	TCP	0	0	SERVER	
casservice3	Up	192.168.1.31	443	SSL	0	0	SERVER	
casservice2	Up	192.168.1.30	443	SSL	0	0	SERVER	
casservice1	Up	192.168.1.29	443	SSL	0	0	SERVER	
offc_webapp_443_1	Up	192.168.1.24	443	SSL	0	0	SERVER	

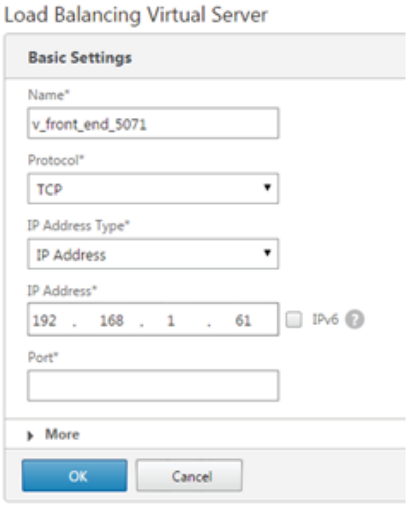
Step 4: Create NetScaler Virtual Servers

After creating the relevant servers and services as described above, you should create virtual serv- ers that will load balance these services. Navigate to Traffic Management>Load Balancing>Virtual Servers, then click Add as shown in the next screenshot.

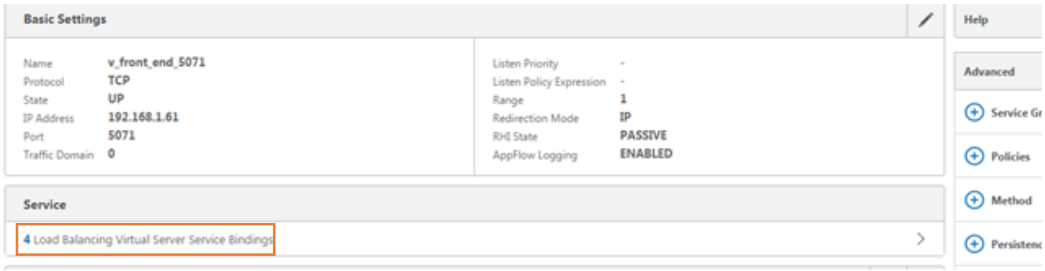


The Load Balancing Virtual Server screen will be displayed. As stated earlier, this configuration should be repeated for all services that are deployed in your Skype for Business environment.

As an example, the virtual server configured below is for the incoming Response Group SIP request handling on port 5071 on the front end server.

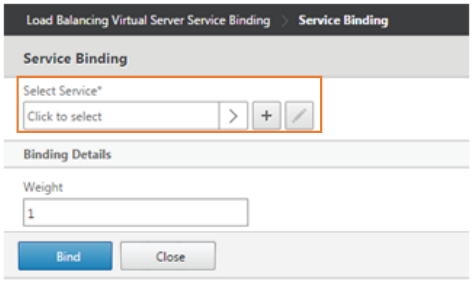


After creating the virtual servers, bind the appropriate services to them by selecting Load Balancer Virtual Server Service Bindings under the Service header as shown below -

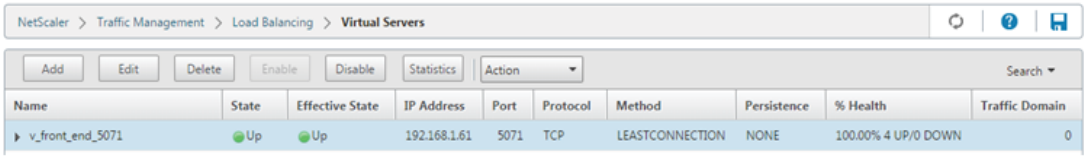


To bind these services, click Add Binding.

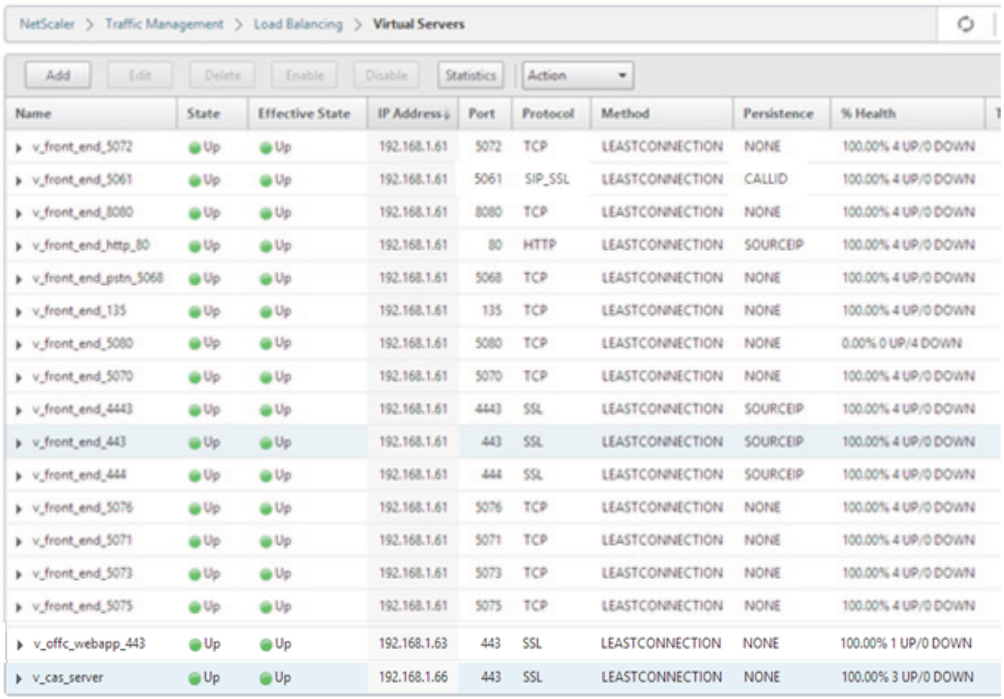
Then, select the appropriate services (created earlier) using the Select Service option.



Once services have been successfully bound, return to the Virtual Servers listing screen and verify that the virtual server is shown as Up, as illustrated below.



After adding the required virtual servers, the listing should include the following entries-



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
v_front_end_5072	Up	Up	192.168.1.61	5072	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_5061	Up	Up	192.168.1.61	5061	SIP_SSL	LEASTCONNECTION	CALLID	100.00% 4 UP/0 DOWN
v_front_end_8080	Up	Up	192.168.1.61	8080	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_http_80	Up	Up	192.168.1.61	80	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 4 UP/0 DOWN
v_front_end_pstn_5068	Up	Up	192.168.1.61	5068	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_135	Up	Up	192.168.1.61	135	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_5080	Up	Up	192.168.1.61	5080	TCP	LEASTCONNECTION	NONE	0.00% 0 UP/4 DOWN
v_front_end_5070	Up	Up	192.168.1.61	5070	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_4443	Up	Up	192.168.1.61	4443	SSL	LEASTCONNECTION	SOURCEIP	100.00% 4 UP/0 DOWN
v_front_end_443	Up	Up	192.168.1.61	443	SSL	LEASTCONNECTION	SOURCEIP	100.00% 4 UP/0 DOWN
v_front_end_444	Up	Up	192.168.1.61	444	SSL	LEASTCONNECTION	SOURCEIP	100.00% 4 UP/0 DOWN
v_front_end_5076	Up	Up	192.168.1.61	5076	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_5071	Up	Up	192.168.1.61	5071	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_5073	Up	Up	192.168.1.61	5073	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_front_end_5075	Up	Up	192.168.1.61	5075	TCP	LEASTCONNECTION	NONE	100.00% 4 UP/0 DOWN
v_offc_webapp_443	Up	Up	192.168.1.63	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN
v_cas_server	Up	Up	192.168.1.66	443	SSL	LEASTCONNECTION	NONE	100.00% 3 UP/0 DOWN

Note: With older NetScaler releases (<10.5.e), the SIP_SSL protocol for the v_director_5061 and v_ front_ end_5061 may not be available. In that case, these virtual servers should be configured with TCP and Source IP persistency.

In the list above, the following IP information is used –

IP Address	Details
192.168.1.61	NetScaler Virtual Server for Front End Servers
192.168.1.62	NetScaler Virtual Server for Director Servers
192.168.1.63	NetScaler Virtual Server for Office Web App Server
192.168.1.66	NetScaler Virtual Server for CAS (Exchange)

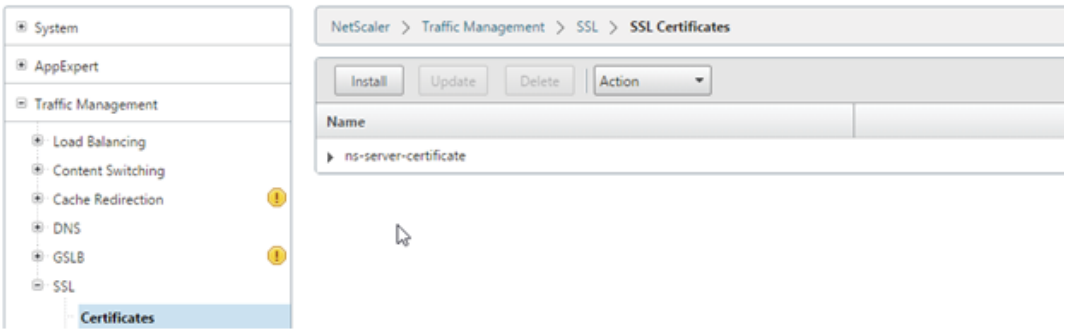
Step 5: Internal DNS Considerations

Below is an example of internal DNS Configuration used while testing in the lab: (please refer to the IP information table in the last section to understand which IP links to which NetScaler virtual server)

FQDN	IP Address
dialin.yourdomain.com	192.168.1.62
meet.yourdomain.com	192.168.1.62
Lyncdiscover.yourdomain.com	192.168.1.62
Owa.yourdomain.com	192.168.1.63
LyncWeb.yourdomain.com	192.168.1.61
LyncWebDir.yourdomain.com	192.168.1.62

Step 6: SSL Certificate Considerations

Create the following server certificates, and then bind them to the appropriate NetScaler virtual servers using the commands shown. You can also do this by navigating to the Certificates section at Traffic Management>SSL using the NetScaler GUI.



Note: These certificates must be created when setting up Skype For Business. You can select these certificates from the Skype for Business Front End and Director Servers and apply them as shown below.

Certificate Attributes:
Subject: CN=Dirpool.yourdomain.com
X509v3 Subject Alternative Name:
DNS:sip.Yourdomain.com, DNS:dir2.yourdomain.com, DNS:Dirpool.yourdomain.com, DNS:Dir1. Yourdomain.com, DNS:dialin.yourdomain.com, DNS:meet.yourdomain.com, DNS:admin. yourdomain.com, DNS:lyncdiscoverInternal.Yourdomain.com, DNS:lyncdiscover.Yourdomain.com Commands to be executed on the NetScaler:

```
add sslcertKeysfb_cert -cert dirpool.pem -key dirpool.pem
bind sslvserver v_director_443 -certkeyNamesfb_cert
bind sslvserver v_director_444 -certkeyNamesfb_cert
bind sslvserver v_director_5061 -certkeyNamesfb_cert
```

(These three virtual servers correspond to Director pool ports 443, 444 and 5061)

Certificate Attributes:
Subject: CN=LyncwebDir.yourdomain.com
X509v3 Subject Alternative Name:
DNS:Dirpool.yourdomain.com, DNS:dialin.yourdomain.com, DNS:meet.yourdomain.com, DNS:admin. yourdomain.com, DNS:Skype for BusinessdiscoverInternal.Yourdomain.com, DNS:Skype for Businessdiscover. Yourdomain.com
Commands to be executed on the NetScaler:

```
addsslcertKeydirwebcert -cert dirweb.pem -key dirwebkey.pem
bind sslvserverv_director_4443 -certkeyNamedirwebcert
```

(This virtual server corresponds to Director pool port 4443)

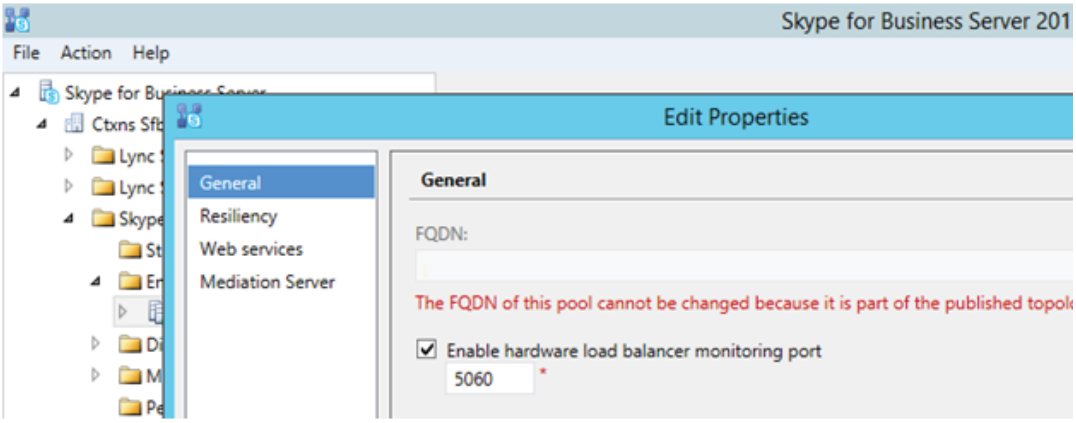
Certificate Attributes:
X509v3 Subject Alternative Name:
DNS:sip.Yourdomain.com, DNS:UCUpdates-r2.yourdomain.com, DNS:UCupdates-r2, DNS:Skype for Businessfe01.Yourdomain.com, DNS:Skype for Businessfe02.Yourdomain.com, DNS:Skype for Businessfe03. Yourdomain.com, DNS:Skype for Businessfe04.Yourdomain.com, DNS:Pool.Yourdomain.com, DNS:dialin. yourdomain.com, DNS:meet.yourdomain.com, DNS:admin. yourdomain.com, DNS:Skype for BusinessdiscoverInternal.Yourdomain.com, DNS:Skype for BusinessWeb.Yourdomain.com, DNS:Skype for Businessdiscover.Yourdomain.com
Commands to be executed on the NetScaler:

```
add sslcertKeypoolupdate_cert -cert pool-update-r2.pem -key pool-update- r2.ky
bind sslvserver v_front_end_443 -certkeyNamepoolupdate_cert
bind sslvserver v_front_end_444 -certkeyNamepoolupdate_cert
bind sslvserver v_front_end_4443 -certkeyNamepoolupdate_cert
bind sslvserver v_front_end_5061 -certkeyNamepoolupdate_cert
```

(These four virtual servers correspond to front end pool ports 443, 444, 4443 and 5061)

Optional: Monitoring Resources

The front-end pool SIP Traffic on port 5061 is encrypted. However, you can optionally enable the unencrypted port 5060 for health monitoring (Note: SIP communication only occurs on the encrypted port, you can choose toenableport 5060 for health monitoring purposes only). This is achieved with the Skype for Business Topology Builder as shown below.



Once this change has been made, publish the topology to enable this port and create the custom NetScaler monitor. When creating this monitor, use SIP_TCP as the protocol for the monitor as the NetScaler appliance supports Extended Content Verification using SIP_TCP. For versions of NetScaler older than 10.5.e, you may use SIP_UDP as the protocol. Optionally, you can create cus- tom monitors for the internal SIP virtual servers.

Load Balancing and Reverse Proxy for External traffic

Load Balancing Edge Pool

For the Edge pool, the NetScaler will serve as the connectivity point to both the internal and exter- nal NICs for multiple edge servers in an array.

- Access Edge: The Access Edge service provides a single, trusted connection point for both out-bound and inbound Session Initiation Protocol (SIP) traffic.
- Web Conferencing Edge: The Web Conferencing Edge service enables external users to join meetings that are hosted on an internal Skype for Business Server 2015 deployment.
- A/V Edge service: The A/V Edge service makes audio, video, application sharing, and file transfer available to external users. Users can add audio and video to meetings that include external participants, and they can communicate using audio and/or video directly with an external user in point-to-point sessions. The A/V Edge service also provides support for desktop sharing and file transfer.
- XMPP Proxy: The XMPP Proxy service accepts and sends extensible messaging and presence pro- tocol (XMPP) messages to and from configured XMPP Federated partners.

HTTPS Reverse Proxy

For Microsoft Skype for Business Server 2015 Edge Server deployments, an HTTPS reverse proxy (i.e. NetScaler) in the perimeter network is required for external clients to access the Skype for Business Server 2015 Web Services (called Web Components in Office Communications Server) on the Director and the user's home pool. A reverse proxy is required because web services are located in the internal Skype for Business Pool; the Skype for Business Edge does not provide these features.

Some of the features that require external access through a reverse proxy include the following:

- Enabling external users to download meeting content for your meetings.
- Enabling external users to expand distribution groups.
- Enabling remote users to download files from the Address Book service.
- Accessing the Skype for Business Web App client.
- Accessing the Dial-in Conferencing Settings webpage.
- Accessing the Location Information service.
- Enabling external devices to connect to Device Update web service and obtain updates.
- Enabling mobile applications to automatically discover and use the mobility (Mcx) URLs from the Internet.
- Enabling the Skype for Business 2015 client, Skype for Business Windows Store app and Skype for Business 2015 Mobile client to locate the Skype for Business Discover (autodiscover) URLs and use the Unified Communications Web API (UCWA).

Mobility

All mobility service traffic goes through the reverse proxy, regardless of the origination point—internal or external. In the case of a single reverse proxy, farm of reverse proxies, or a device acting as a reverse proxy, an issue can arise when the internal traffic is egressing through an interface and attempting to immediately ingress on the same interface. This often leads to a security rule viola- tion known as spoofing, or TCP packet spoofing. Hair pinning (the egress and immediate ingress of a packet or series of packets) must be allowed in order for mobility to function. One way to resolve this issue is to use a reverse proxy separate from the firewall (the spoofing prevention rule should always be enforced at the firewall). The hairpin can occur at the external interface of the reverse proxy instead of the firewall external interface. Spoofing is detected at the firewall, and rules are relaxed at the reverse proxy, thereby allowing the hairpin required by mobile traffic.

Federations & XMPP Partners

Federation, public instant messaging connectivity and Extensible Messaging and Presence Protocol (XMPP) define a different class of external users – Federated users. Users of a federated Skype for Business Server deployment or XMPP deployment have access to a limited set of services and are authenticated by the external deployment. Remote users are members of your Skype for Business Server deployment and have access to all services offered.

Public instant messaging connectivity is a special type of federation that allows a Skype for Business Server client to access configured public Instant Messaging partners using Skype for Business. Instant messaging connectivity is supported between Skype for Business and Skype users. (More details are provided at https://technet.microsoft.com/en-us/library/dn705313.aspx in the Clients and Interoperability Matrix)

A public instant messaging connectivity configuration allows Skype for Business user's access to public instant messaging connectivity users by:

- IM and Presence
- Visibility of public instant messaging connectivity contacts in Skype for Business client
- Person to person IM conversations with contacts
- Audio and video calls with Windows Live users

Skype for Business Server federation defines an agreement between your Skype for Business Server deployment and other Office Communications Server 2007 R2 or Lync deployments. A Skype for Business Server federated configuration provides Skype for Business users with access to federated users by:

- IM and Presence
- Creation of federated contacts in the Skype for Business client

XMPP federation defines an external deployment based on the eXtensible Messaging and Presence Protocol. An XMPP configuration provides Skype for Business users with access to allowed XMPP domain users by:

- IM and Presence – person to person only
- Creation of XMPP federated contacts in the Skype for Business client

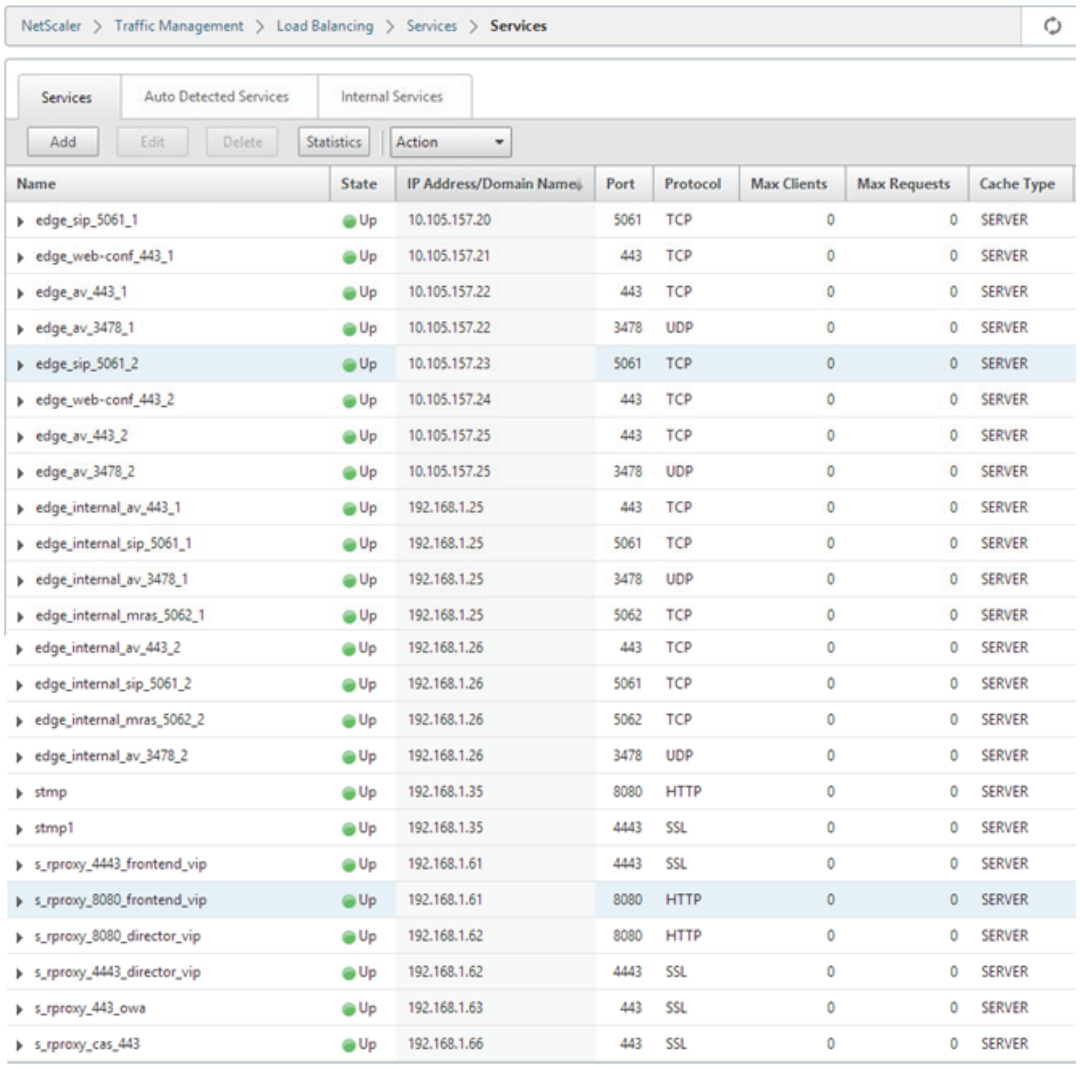
Load balancing external traffic

Lab Setup - External

Role	FQDN	IP Network Interfaces	Additional Information
Skype for Business Edge Internal Server	Edge1.yourdomain.com	192.168.1.x	
Skype for Business Edge External Server 1	sfbEdge01.yourdomain. com	192.168.1.x	
Skype for Business Edge External Server 1	sfbEdge02.yourdomain. com	192.168.1.x	
NetScaler		10.105.157.x	

Step 1: Create Services

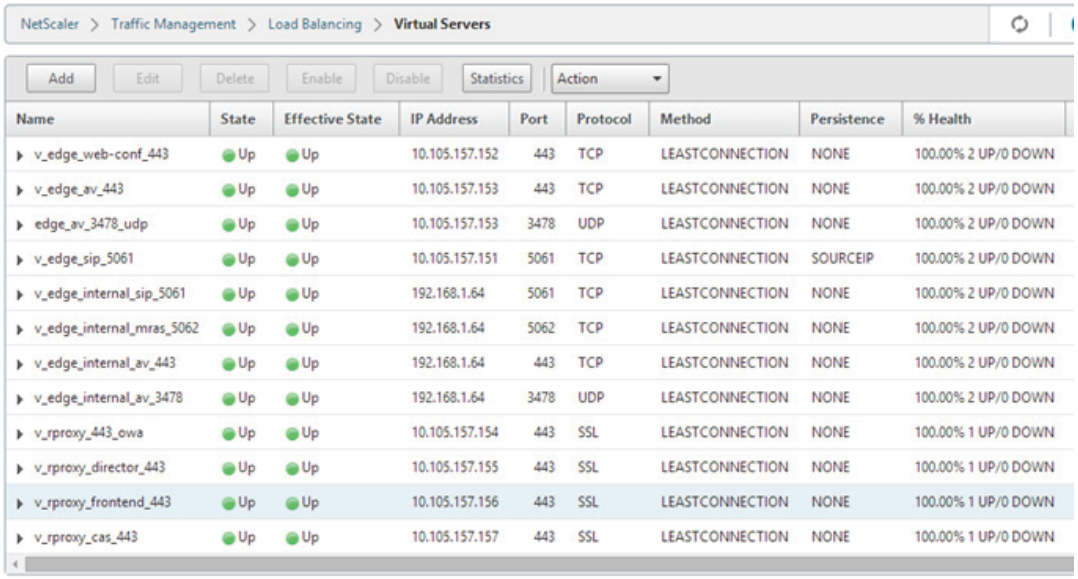
The steps for configuration here are similar to the steps used for the internal deployment. Refer to the configuration tables provided earlier and configure the external deployment services using the same process. You should see the following virtual servers in your deployment.



Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type
edge_sip_5061_1	Up	10.105.157.20	5061	TCP	0	0	SERVER
edge_web-conf_443_1	Up	10.105.157.21	443	TCP	0	0	SERVER
edge_av_443_1	Up	10.105.157.22	443	TCP	0	0	SERVER
edge_av_3478_1	Up	10.105.157.22	3478	UDP	0	0	SERVER
edge_sip_5061_2	Up	10.105.157.23	5061	TCP	0	0	SERVER
edge_web-conf_443_2	Up	10.105.157.24	443	TCP	0	0	SERVER
edge_av_443_2	Up	10.105.157.25	443	TCP	0	0	SERVER
edge_av_3478_2	Up	10.105.157.25	3478	UDP	0	0	SERVER
edge_internal_av_443_1	Up	192.168.1.25	443	TCP	0	0	SERVER
edge_internal_sip_5061_1	Up	192.168.1.25	5061	TCP	0	0	SERVER
edge_internal_av_3478_1	Up	192.168.1.25	3478	UDP	0	0	SERVER
edge_internal_mras_5062_1	Up	192.168.1.25	5062	TCP	0	0	SERVER
edge_internal_av_443_2	Up	192.168.1.26	443	TCP	0	0	SERVER
edge_internal_sip_5061_2	Up	192.168.1.26	5061	TCP	0	0	SERVER
edge_internal_mras_5062_2	Up	192.168.1.26	5062	TCP	0	0	SERVER
edge_internal_av_3478_2	Up	192.168.1.26	3478	UDP	0	0	SERVER
stmp	Up	192.168.1.35	8080	HTTP	0	0	SERVER
stmp1	Up	192.168.1.35	4443	SSL	0	0	SERVER
s_rproxy_4443_frontend_vip	Up	192.168.1.61	4443	SSL	0	0	SERVER
s_rproxy_8080_frontend_vip	Up	192.168.1.61	8080	HTTP	0	0	SERVER
s_rproxy_8080_director_vip	Up	192.168.1.62	8080	HTTP	0	0	SERVER
s_rproxy_4443_director_vip	Up	192.168.1.62	4443	SSL	0	0	SERVER
s_rproxy_443_owa	Up	192.168.1.63	443	SSL	0	0	SERVER
s_rproxy_cas_443	Up	192.168.1.66	443	SSL	0	0	SERVER

Step 2: Configure Virtual Servers

As configured for the internal deployment, configure virtual servers corresponding to the services created in the last step. You should have the following virtual servers (or a subset, depending on the Skype for Business services setup in your environment)



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
v_edge_web-conf_443	Up	Up	10.105.157.152	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_edge_av_443	Up	Up	10.105.157.153	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
edge_av_3478_udp	Up	Up	10.105.157.153	3478	UDP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_edge_sip_5061	Up	Up	10.105.157.151	5061	TCP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN
v_edge_internal_sip_5061	Up	Up	192.168.1.64	5061	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_edge_internal_mras_5062	Up	Up	192.168.1.64	5062	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_edge_internal_av_443	Up	Up	192.168.1.64	443	TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_edge_internal_av_3478	Up	Up	192.168.1.64	3478	UDP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
v_rproxy_443_owa	Up	Up	10.105.157.154	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN
v_rproxy_director_443	Up	Up	10.105.157.155	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN
v_rproxy_frontend_443	Up	Up	10.105.157.156	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN
v_rproxy_cas_443	Up	Up	10.105.157.157	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN

External DNS Considerations

Below is an example of external DNS Configuration used while testing in the lab:

FQDN	IP Address
Owa.yourdomain.com	10.105.157.154:443
Lyncdiscover.yourdomain.com	10.105.157.155:443
Lyncweb.yourdomain.com	10.105.157.156:443
LyncWebDir.yourdomain.com	10.105.157.155:443
Dialin.yourdomain.com	10.105.157.155:443
Meet.yourdomain.com	10.105.157.155:443
Mail.yourdomain.com	10.105.157.157:443
Sip.yourdomain.com	10.105.157.151:5061
webconf.yourdomain.com	10.105.157.152:443
av.yourdomain.com	10.105.157.153:443

(Refer to the last screenshot for details on which IP corresponds to which virtual server)

SSL Certificate Considerations

Create the below Server Certificate using a Public Trusted CA with Subject name and Subject alter- native names as shown below. This is necessary as an Internal CA would not be trusted by external clients.
Certificate Attributes:
Subject: CN=*.yourdomain.com
Subject Alternative Name:
DNS:dialin.yourdomain.com,
DNS:meet.yourdomain.com,
DNS:Skype for Businessdiscover.yourdomain.com,
DNS:Skype for Businesswebdir.yourdomain.com,
DNS:admin.yourdomain.com,
DNS:sip.yourdomain.com,
DNS:webconf.yourdomain.com,
DNS:av.yourdomain.com,
DNS:owa.yourdomain.com,
DNS:Skype for Businessweb.yourdomain.com,
DNS:*.yourdomain.com
(Example: The above cert is generated with rp.pem and its corresponding private key rpkey.pem)
Commands to be executed on the NetScaler:
Add this cert inside the NS and bind it with the External VIPs as shown below -

```
add sslcertKeyrpcert -cert rp.pem -key rpkey.pem
bind sslvserverv_rproxy_443_owa -certkeyNamerpcert
bind sslvserver v_rproxy_director_443 -certkeyNamerpcert
bind sslvserver v_rproxy_frontend_443 -certkeyNamerpcert
```

Benefits of using a hardware load balancer

Skype for Business 2015 allows load balancing of network traffic that is unique to Skype for Business such as SIP and media traffic. Basic DNS load balancing can also support Front End, Edge Server, Director, and stand-alone Mediation Server pools. While DNS load balancing is lean and easy to maintain, this simplicity comes at the cost of availability, security and quality of service for end users.

The benefits of using a hardware load balancer in your Skype for Business 2015 deployment are -

1. Persistency of HTTP traffic

Though IM traffic is SIP based, data such as Address books,Shared content, Web based meeting connectivity, Group expansion and Device updates is HTTP-based. HTTP traffic is session oriented and therefore needs persistence. DNS load balancing does not support persistency and deploying a single server creates a single point of failure.

a. Hardware load balancers can support load balancing HTTP traffic with persistence

b. NetScaler provides industry leading HTTP load balancing, monitoring and persistence capabilities

c. Leverage connection multiplexing for optimal server utilization

d. Improve performance by enabling advanced compression and caching features

2. Quick automatic failure

DNS load balancing relies on the client or endpoint to determine the availability of servers in each pool, which is more reactive than preventative. A query for an FQDN provides a list of IPs for all pool members. If a client connects to a failed node, only then will it will resort to the next node in the list, which can lead to delays. Failed nodes must be manually removed from list.

a. A hardware load balancers provide monitors to check availability. This provides a proactive failure management and detection

b. Leverage application aware monitors of NetScaler for intelligent monitoring

c. NetScaler GSLB provides a disaster recovery solution across multiple data centers distributed across geographical locations.

3. Seamless integration for federation cases

OCS 2007 does not support DNS load balancing. Public IM services such as Skype, Google Talk etc., generally do not support DNS load balancing. DNS load balancing on your Edge Servers causes an interruptionin failover capabilitiesand increases the difficulty involved in interenterprise integration. These scenarios will work as long as all Edge Servers in the pool are up and running, but if one Edge Server is unavailable, any requests for these scenarios that are sent to it will fail, instead of routing to another Edge Server.

a. Hardware load balancers provide seamless integration and provide transparent load balancing and monitoring.

4. Seamless integration for Exchange Server Unified Management – Microsoft recommends hard- ware load balancing for Exchange.

5. Support for telephony equipment

Call failure rates are high when using DNS load balancing for the mediation server role with an IPBX that does not understand DNS LB.

Conclusion

A leading application delivery solution, Citrix NetScaler exceeds Microsoft's external load balancer recommendations for Skype for Business deployments. Working closely with Microsoft's engineer- ing and test teams, Citrix has designed NetScaler to optimize the delivery of traffic, achieving significant TCO savings while providing increased availability, capacity, performance, security and manageability.

To learn more about how NetScaler can bring these benefits to Skype for Business installations or address other application delivery requirements, please visit http://www.citrix.com.

Appendix

Product versions used during testing

Product	Version
Microsoft Skype for Business	Skype For Business Server
SQL Server (SQL Server 2012)	SQL Server 2014
Citrix NetScaler	NetScaler 11.0

Skype for Business PowerShell Commands

Product	Version
Export Configuration for Edge Servers	Export-CsConfiguration –FileName<path/filename>
Update Address Book	Update-CsAddressBook
Verify Status of Replication	Get-CsManagementStoreReplicationStatus
Display Access Edge Configuration	Get-CsAccessEdgeConfiguration

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China