Application Note

Lync 2010 deployment guide

Document version:	v1.2
Last update:	12th December 2013
Lync server:	2010
ALOHA version:	5.5 and above

RULE YOUR NETWORK!®

EXCELIANCE

Contents

1 Introduction

1.1 About Exceliance

Exceliance is a software company, editing the Application Delivery Controller called **ALOHA Load-Balancer**. Headquartered in Jouy-en-Josas (Yvelines), all its team (including R&D and technical support) is based in France.
Exceliance currently has around 200 customers in the banking, retail groups, energy and e-commerce industries and the public sector. Exceliance solutions are also used by many hosting providers.
The **ALOHA Load-balancer** is designed to improve performance, guarantee quality of service and ensure the availability of critical business applications, by dynamically balancing flows and queries on the company's various servers.

1.2 About ALOHA Load-balancer

The **ALOHA Load-Balancer** is designed to load-balance at layer 4 and control application delivery at layer 7. It is designed to integrate simply and quickly into any environment or architecture. The main **ALOHA Load-Balancer** benefits are:

- Guarantee applications and services availability as well as improve web application performance
- Makes infrastructures scalable and reliable
- Simplifies architecture: IPv6 frontend, SSL offloading, layer 7 routing
- Protect the infrastructure against DDOS and any type of attacks

Developed using HAProxy open source load balancing software, Exceliance solutions are known for their processing performance, reliability and wealth of features. Offered at more affordable prices than other commercial solutions, they are easy to deploy and to administer.
ALOHA Load-balancer is available either as a physical appliance or as a Virtual Appliance. The Virtual appliance can run on top of any hypervisor available on the market.

1.3 About this guide

The guide provides configuration templates to setup the **ALOHA Load-Balancer** for **Microsoft Lync 2010**.
The latest version of this guide can be downloaded from Exceliance website: http://www.exceliance.fr/.

1.4 Appliance supported

All **ALOHA Load-Balancer** appliances can be used with **Microsoft Lync 2010**. (physical and virtual ones).

1.5 Aloha firmware versions supported

ALOHA 4.2 and above are supported to load-Balance **Microsoft Lync 2010**.

the configuration templates provided in this guide applies to the latest ALOHA Long Term Support 5.5 branch. For earlier version, the configuration may be slightly different. Please contact Exceliance Pre-sales team for help and information.

1.6 Microsoft Lync version supported

ALOHA load-balancer can be used with the following versions of **Microsoft Lync**:

- Microsoft Lync 2010

1.7 Document history

- 2013-11-08: template updates, Lync introduction updated
- 2013-11-08: Minor typo changes
- 2013-01-24: Initial Version

1.8 Disclaimer

The **Lync 2010** configuration tips which might be provided in this guide are purely informational. For more information about **Microsoft Lync 2010** tools and how to use them, please refer to Microsoft web site which is fully and properly documented.

2 Lync 2010 introduction

2.1 Description

Microsoft Lync Server 2010 (previously known as Microsoft Office Communications Server, OCS) is an enterprise level communications server application, providing services such as instant messaging, VoIP, conferences (audio, video and web conferencing) and Public Switch Telephone Network (PSTN) or SIP connectivity.
It can be used in an enterprise network or can be connected to the outside world, for external communication.

2.2 Server roles

The table below summarizes the different **Lync 2010** server roles and provides useful information from a load-balancing point of view.

Role name	Description
Front End	Core server role, it runs many Lync Server services. This is role is **required** for **Lync 2010**. High Availability can be achieved with the **ALOHA Load-Balancer**.
Edge	Allow 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 off-site, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. This role also enables connectivity to public IM connectivity services, including Windows Live, AOL, Yahoo! and Google Talk. High Availability can be achieved with the **ALOHA Load-Balancer**.
Director	Used in collaboration with **Edge Servers**. **Director Servers** authenticates external users, before passing their traffic to the internal servers. Directors can also be deployed with **Front End** pools to improve performance: the **Director** routes requests to the correct **Front End** pool. High Availability can be achieved with the **ALOHA Load-Balancer**. This is a **required** role when **Edge Servers** are deployed.
Audio/Video Conferencing	Provides Audio / Visual conferencing functionality to Lync clients. One can use a pool of **A/V Conferencing** servers for high-availability. This role is can be installed on the **Front End** Server or standing on its own server.

Role name	Description
Mediation	Enables Enterprise Voice and dial-in conferencing. Mediation Server translates signaling between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. This role is can be installed on the **Front End** Server or standing on its own server. High Availability can be achieved with the **ALOHA Load-Balancer**.
Communicator Web Access	shortened to **CWA** Allows users who do not have a Lync client to use the Lync Server services. It is an extension from **Lync 2010** and cannot be run separately. This role is can be installed on the **Front End** Server or standing on its own server.
Monitoring	Collects information from the Lync infrastructure and ability to run reports for administrator. This information can be used to help to provide the best possible media experience for users to plan future growth. This role is can be installed on the **Archiving** Server or standing on its own server. **This role is outside the Load-Balancing scope**
Archiving	Allows archiving of IM communications and meeting content. Only required if you have legal concerns. This role is can be installed on the **Monitoring** Server or standing on its own server. **This role is outside the Load-Balancing scope**
Back End	It can host various SQL Server databases to keep track of Lync's configuration and state information. Microsoft recommends using an **SQL cluster** for high availability. This is role is **required** for **Lync 2010**. **This role is outside the Load-Balancing scope**

2.3 Load Balancing Lync 2010

Lync 2010 supports two ways of load balancing:

1. Domain Name System (DNS)
2. Hardware Load Balancing (HLB)

2.3.1 DNS Load Balancing

Lync 2010 DNS load balancing is implemented on the client side: when a Lync 2010 client wants to get connected to a Lync infrastructure, it queries the DNS which will provide it all member addresses. The client then attempts to establish a TCP connection to one of these IP addresses. If it fails, the client tries the next IP address.
If the client can't get successfully connected on any server running IP address provided by the DNS, then an error is returned to the client, mentioning no **Lync 2010** servers are available.

Services relying on HTTP/HTTPs are session state oriented and can't use the DNS load-balancing method.
In this case a Hardware Load Balancer must be used.

2.3.2 Hardware Load Balancing (HLB)

As explained in the previous chapter, hardware based load balancing is required for Web based services. That said, DNS and HLB based load-balancing can be used together or the HLB can be used alone to load-balance all **Lync 2010** services.

2.3.3 Why using a Load-Balancer for Lync 2010?

- Fault tolerance is limited and failover can take much longer than when using a **Load-Balancer**
- The **Load-Balancer** can also cover the Reverse-Proxy features needed by **Lync 2010**
- The **Load-Balancer** allows graceful shutdown of servers by draining traffic to it without cutting any connections
- DNS roundrobin is not load-balancing while the **Load-Balancer** can perform smooth and smart load-balancing

That said, you have to note that a **Load-Balancer** may add complexity in **Lync 2010** deployment.

2.3.4 Hardware Load-Balancer deployment mode

The **ALOHA Load-Balancer** can be used in the mode below:

- Layer 7 reverse-proxy, also known as source NAT or Full NAT. Easiest integration, no architecture modification required.
- Layer 7 Transparent proxy, same as reverse-proxy mode but client IP is not hidden. The HLB must be the server's default gateway
- Layer 4 Destination NAT. The HLB must be the server's default gateway. The HLB acts as a router.
- Layer 4 Direct Server Return, also known as gateway mode. The HLB Virtual IP must be configured on a server loopback. The HLB acts as a router.
  Lync 2010 is not compatible with this mode.
- Layer 4 IPIP tunnel. The HLB Virtual IP must be configured on a server loopback and the server

must be compatible with IPIP tunnels. The HLB acts as a router.
Lync 2010 is not compatible with this mode.

In this guide, all the TCP based services will be load-balanced in reverse-proxy mode, labelled **Layer 7** mode in the ALOHA GUI. UDP based services will be load-balanced with the Layer 4 Destination NAT mode, labelled **Layer 4** in the ALOHA GUI

2.4 Lync 2010 services summary

2.4.1 External services

2.4.1.1 Edge server pool

Port	Protocols	Service purpose
443	TCP / STUN	SIP
443	TCP / STUN	Conferencing
443	TCP / STUN	Audio/Video TCP (failover from UDP)
3478	UDP / STUN	Audio/Video UDP
5061	TCP / TLS / SIP	Access Edge federation

Because 3 different services require TCP port 443, you must use 3 different public IP addresses. Fortunately, the **Conferencing** and **Audio/Video TCP** services can run on different ports, allowing you to lower your deployment requirements in term of Public IP addresses.

2.4.1.2 Director servers

Port	Protocols	Service purpose
443	TCP / HTTPs	web services

The **Load-Balancer** replaces the **Reverse-proxy** in this case

2.4.1.3 Front End servers

Port	Protocols	Service purpose
443	TCP / HTTPs	mobile client access, autodiscover

The **Load-Balancer** replaces the **Reverse-proxy** in this case

2.4.2 Internal services

2.4.2.1 Edge server pool

Port	Protocols	Service purpose
443	TCP / STUN	Used for SIP/TLS communication for external users accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions
3478	UDP / STUN	Used for STUN/UDP inbound and outbound media exchange.
5061	TCP / MTLS / SIP	SIP/TLS to edge
5062	TCP / MTLS / SIP	Edge A/V authorization
8057	TCP / MTLS	Used to listen for Persistent Shared Object Model (PSOM) connections from client

2.4.2.2 Director servers

Port	Protocols	Service purpose
80	TCP / HTTP	various HTTP services
443	TCP / HTTPS	Communication between **Directors** and **Front End**
444	TCP / HTTPS	Communication between **Directors** and **Front End**
4443	TCP / HTTPS	External Web Services from Reverse Proxies
5060	TCP / SIP	Optionally used for static routes to trusted services, such as remote call control servers
5061	TCP / TLS / SIP	Used for internal communications between servers and for client connections
8080	TCP / HTTP	External Web Services from Reverse Proxies

2.4.2.3 Front End servers

Port	Protocols	Service purpose
135	TCP / DCOM	Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization
443	TCP / HTTPs	Internal web services
444	TCP / HTTPs	Used for communication between the Focus (the Lync Server component that manages conference state) and the individual servers
4443	TCP / HTTPs	External web services from reverse proxies
5061	TCP / TLS / SIP	Used by Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS).
5065	TCP	Used for incoming SIP listening requests for application sharing
5069	TCP	Used by Quality of Experience (QoE) agent on the Front End Server

Optional services:

Port	Protocols	Service purpose
80	TCP / HTTP	Various HTTP based Services
448	TCP	Used for call admission control by the Lync Server Bandwidth Policy Service
5060	TCP / SIP	Unsecured SIP Traffic
5071	TCP / SIP	Used for incoming SIP requests for the Response Group application
5072	TCP / SIP	Used for incoming SIP requests for Microsoft Lync 2010 Attendant (dial in conferencing)
5073	TCP / SIP	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing)
5074	TCP / SIP	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing)
5075	TCP / SIP	Incoming SIP requests for the Call Park application
5076	TCP / SIP	Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing)
5080	TCP	Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic
8080	TCP / HTTPs	External web services from reverse proxies

2.4.2.4 Mediation servers

Port	Protocols	Service purpose
5067	TCP / TLS / SIP	Used for incoming SIP requests from the PSTN gateway
5068	TCP / TLS / SIP	Used for incoming SIP requests from the PSTN gateway
5070	TCP / SIP	Incoming requests from the Front End Server

The **Mediation** role is usually hosted on the **Frontend** server

2.5 Persistence

Most **Lync 2010** services are compatible with source IP persistence: actually, only **Mobility services**, when enabled through the Forefront TMG reverse-proxies, and Communicator Web applications must use application layer persistence, such as **HTTP Cookie**.
Since Lync 2010 does not allow SSL offloading, when performing Cookie based persistence, the Load-Balancer must decypher the incoming traffic and cypher the outgoing traffic.
Fortunately, the **ALOHA Load-Balancer** can do this easily for you.

2.6 Timeout settings

In **Lync 2010**, the TCP idle timeout is setup to 20 minutes by default. It is recommended to setup a timeout slightly higher in your configuration.
In the configuration templates provided in this guide, we'll use 30 minutes timeout (or 1800 seconds)

for TCP based services.

2.7 Lync 2010 Web Services

In order to publish Web Services in a **Lync 2010** infrastructure, it is required to use Microsoft Forefront Threat Management Gateway (TMG) 2010.
Microsoft recommends that all Web Services in all pools should be published. One publishing rule for each Front End pool and Director pool is required.

When **Director Servers** are deployed, the reverse proxies should listen for HTTP/HTTPS requests to the simple URLs and should proxy them to the external Web Services virtual directory on the **Director** pool.

Forefront TMG configuration and load-balancing is outside the scope of this guide.

2.8 Mobility Web Services

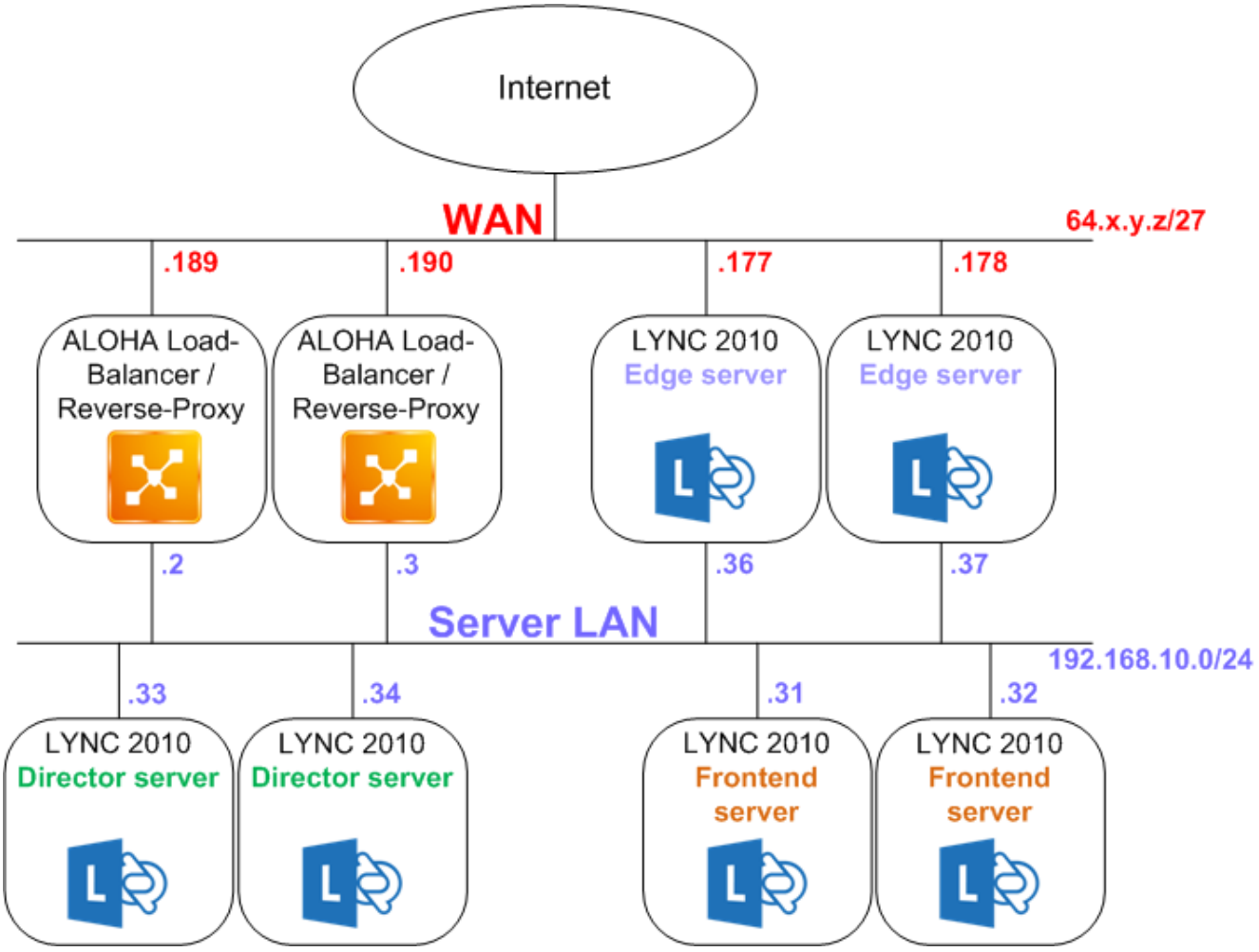
When load-balancing Mobility web services, we must provide cookie based persistence: SSL bridging is mandatory, since clients get connected over an SSL connection and the Lync servers expect SSL connections as well.
SSL bridging related documentation is provided at the end of this document.

2.9 Microsoft documentation about Lync 2010 Load-Balancing

- Hardware Load Balancer Requirements:
  `http://technet.microsoft.com/en-us/library/jj656815.aspx`
- Setting Up Reverse Proxy Servers:
  `http://technet.microsoft.com/en-us/library/gg398069.aspx`
- Load Balancing Requirements:
  `http://technet.microsoft.com/en-us/library/gg615011.aspx`
- Components Required for External User Access:
  `http://technet.microsoft.com/en-us/library/gg425779.aspx`
- Ports and Protocols for Internal Servers:
  `http://technet.microsoft.com/en-us/library/gg398833.aspx`
- Port Summary - Scaled Consolidated Edge with Hardware Load Balancers:
  `http://technet.microsoft.com/en-us/library/gg398739.aspx`
- Microsoft Lync Server 2010 Protocol Workloads Poster:
  `http://www.microsoft.com/en-us/download/details.aspx?id=6797`

3 Lync infrastructure and ALOHA Load-Balancer

The diagram below shows an example of **ALOHA Load-Balancer** deployment in a **Lync 2010** infrastructure:



The main components are:

- One cluster of **ALOHA load-balancer**, plugged in the public DMZ and in the LAN. It also assumes the **Reverse-Proxy** feature.
- A pool of **Lync 2010 Edge servers**, in the public DMZ and in the LAN
- A pool of **Lync 2010 Director servers**, in the LAN
- A pool of **Lync 2010** servers with enterprise roles: **Front End**, **AV/V Conferencing** and **Mediation**

Any other roles, such as **Archiving** and **Monitoring** can be installed in the LAN on a dedicated server..

You could also use 2 clusters, one for the public DMZ and one for the LAB to improve security and DMZ isolation.

3.1 External services

3.1.1 Edge pool

The Virtual IPs and Services concerning **External Edge Pool** are configured on the **ALOHA Cluster** public interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
64.x.y.174	443 / TCP	Layer 7	SIP
64.x.y.174	5061 / TCP	Layer 7	SIP federation
64.x.y.174	5062 / TCP	Layer 7	Audio / Video TCP
64.x.y.174	5063 / TCP	Layer 7	Conferencing

The required deployment mode for **Edge servers** is **transparent proxy**. This means the **Edge servers** default gateway must be the **Aloha Load-Balancer**.

In normal case, 3 Public IPs are required because 3 services must listen on port 443: Access, Web conference and A/V. In our lab, we chose to use a single IP but use 3 different TCP ports.

3.1.2 Director pool

The Virtual IPs and Services concerning **Director Pool** external web services are configured on the **ALOHA Cluster** public interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
64.x.y.173	443 / HTTPS	Layer 7	External web services

In this case, the **ALOHA Load-Balancer** acts as a **Reverse-Proxy**

3.1.3 Front End pool

The Virtual IPs and Services concerning Front End Pool external web services are configured on the **ALOHA Cluster**, on its public interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
64.x.y.176	443 / HTTPS	Layer 7	External web services

In this case, the **ALOHA Load-Balancer** acts as a **Reverse-Proxy**

3.2 Internal services

3.2.1 Edge pool

The Virtual IPs and Services concerning **Internal Edge Pool** are configured on the **ALOHA Cluster** LAN interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
192.168.10.8	443 / TCP	Layer 7	SIP TLS communication
192.168.10.8	5061 / TCP	Layer 7	SIP/TLS to Edge
192.168.10.8	5062 / TCP	Layer 7	Audio / Video TCP
192.168.10.8	8057 / TCP	Layer 7	PSOM

3.2.2 Director pool

The Virtual IPs and Services concerning **internal Director Pool** services is configured on the **ALOHA Cluster** LAN interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
192.168.10.7	443 / HTTPS	Layer 7	Directors / frontends communication
192.168.10.7	444 / HTTPS	Layer 7	Directors / frontends communication
192.168.10.7	4443 / HTTPS	Layer 7	Web services
192.168.10.7	5060 / SIP	Layer 7	SIP communication
192.168.10.7	5061 / SIP	Layer 7	TLS SIP communication

3.2.3 Front End pool

TCP based Services:
The Virtual IPs and Services concerning **internal Front End Pool** services is configured on the **ALOHA Cluster** LAN interface.
These services are:

Virtual IP	Port / Protocol	Mode	Service name
192.168.10.6	80 / HTTP	Layer 7	Internal web services
192.168.10.6	135 / TCP	Layer 7	DCOM and RPC
192.168.10.6	443 / HTTPS	Layer 7	Internal web services
192.168.10.6	444 / HTTPS	Layer 7	Internal web services
192.168.10.6	4443 / HTTPS	Layer 7	External web services
192.168.10.6	5060 / TCP	Layer 7	unsecured SIP
192.168.10.6	5061 / TCP	Layer 7	TLS SIP communication
192.168.10.6	5065 / TCP	Layer 7	SIP Application sharing
192.168.10.6	5069 / TCP	Layer 7	SIP QoE
192.168.10.6	5071 / TCP	Layer 7	SIP Response group service
192.168.10.6	5072 / TCP	Layer 7	SIP Conferencing attendant
192.168.10.6	5073 / TCP	Layer 7	SIP Conferencing announcement
192.168.10.6	5074 / TCP	Layer 7	SIP outside voice control
192.168.10.6	5075 / TCP	Layer 7	SIP for call park application
192.168.10.6	5076 / TCP	Layer 7	SIP dial-in conferencing
192.168.10.6	8080 / HTTP	Layer 7	Internal web services

Since the **Frontend servers** also hosts the **Mediation** role, the following ports should be conigured as well:

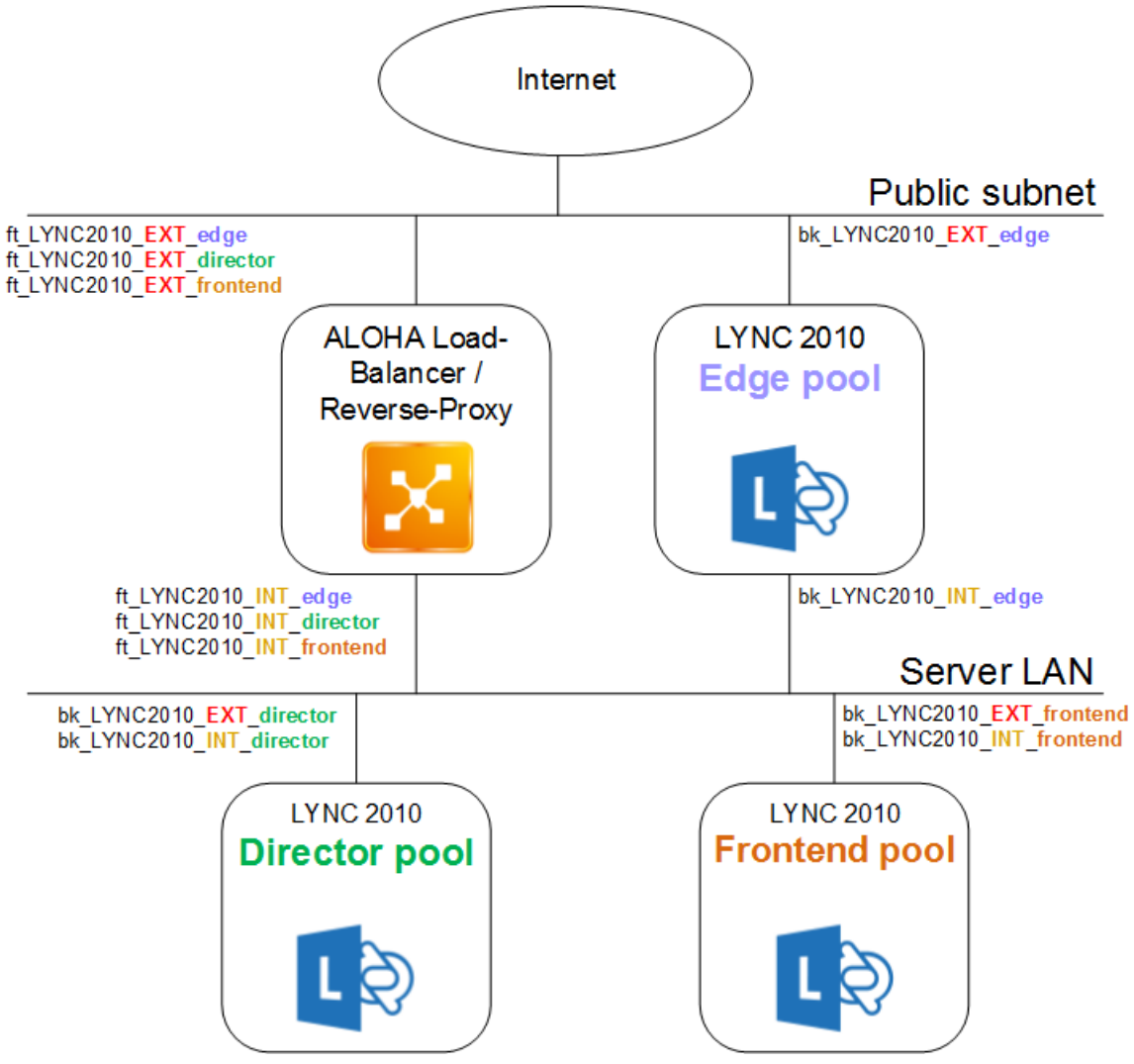
Virtual IP	Port / Protocol	Mode	Service name
192.168.10.6	5067 / TCP	Layer 7	SIP request from PSTN gateway
192.168.10.6	5068 / TCP	Layer 7	SIP request from PSTN gateway
192.168.10.6	5070 / TCP	Layer 7	Incoming request from Frontend servers

4 ALOHA Load-Balancer configuration templates for Lync 2010

Just copy / paste the configuration example below and update them accordingly to your IP addressing scheme.

4.1 HAProxy configuration diagram

The diagram below explains how the HAProxy configuration is setup.
Basically, **EXTERNAL** frontends listen on public interfaces and **INTERNAL** frontends listen on the server lan interface.
The diagram show the name of each frontend and backend in use:



4.2 Default section

It is recommended to setup a default section dedicated to **Lync 2010**.
To be added in the **LB Layer 7** GUI tab:

```
######## Default values for all entries till next defaults section
defaults LYNC2010
  log global
  option tcplog
  option tcpka
  option dontlognull      # Do not log connections with no requests
  option redispatch       # Try another server in case of connection failure
  option contstats        # Enable continuous traffic statistics updates
  option socket-stats
  retries 3               # Try to connect up to 3 times in case of failure
  timeout connect 5s      # 5 seconds max to connect or to stay in queue
  timeout queue 30s       # 30 seconds max queued on load balancer
  timeout tarpit 1m       # tarpit hold tim
  backlog 10000           # Size of SYN backlog queue
```

4.3 External services

4.3.1 Edge pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_EXT_edge
 mode tcp
 bind 64.x.y.174:443 defer-accept name sip
 bind 64.x.y.174:5061 defer-accept name sip-federation
 bind 64.x.y.174:5062 defer-accept name audio_video_tcp
 bind 64.x.y.174:5063 defer-accept name conferencing
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_EXT_edge

backend bk_LYNC2010_EXT_edge
 mode   tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 source 0.0.0.0 usesrc clientip
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lyed1 64.x.y.177 weight 10 check observe layer4 port 443
 server 2010lyed2 64.x.y.178 weight 10 check observe layer4 port 443
```

4.3.2 Director pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_EXT_director
 mode tcp
 bind 64.x.y.173:443 defer-accept name web_services
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_EXT_director

backend bk_LYNC2010_EXT_director
 mode   tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lydir1 192.168.10.33:4443 weight 10 check observe layer4
 server 2010lydir2 192.168.10.34:4443 weight 10 check observe layer4
```

4.3.3 Front End pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_EXT_frontend
 mode tcp
 bind 64.x.y.176:443 defer-accept name web_services
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_EXT_frontend

backend bk_LYNC2010_EXT_frontend
 mode  tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lyfe1 192.168.10.31:4443 weight 10 check observe layer4
 server 2010lyfe2 192.168.10.32:4443 weight 10 check observe layer4
```

4.4 Internal services

4.4.1 Edge pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_INT_edge
 mode tcp
 bind 192.168.10.8:443 name https
 bind 192.168.10.8:5061 name sip
 bind 192.168.10.8:5062 name av_tcp
 bind 192.168.10.8:8057 name webconf_NOTNEEDED
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_INT_edge

backend bk_LYNC2010_INT_edge
 mode tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lyed1 192.168.10.36 weight 10 check observe layer4 port 5061 check-ssl
 server 2010lyed2 192.168.10.37 weight 10 check observe layer4 port 5061 check-ssl
```

4.4.2 Director pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_INT_director
 mode tcp
 bind 192.168.10.7:80 name http
 bind 192.168.10.7:443 name dir_fe_communication
 bind 192.168.10.7:444 name dir_fe_communication
 bind 192.168.10.7:4443 name web_services
 bind 192.168.10.7:5061 name sip
 bind 192.168.10.7:8080 name web_services
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_INT_director

backend bk_LYNC2010_INT_director
 mode tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lydir1 192.168.10.33 weight 10 check port 5061 observe layer4 check-ssl
 server 2010lydir2 192.168.10.34 weight 10 check port 5061 observe layer4 check-ssl
```

4.4.3 Front End pool

To be added in the **LB Layer 7** GUI tab:

```
frontend ft_LYNC2010_INT_frontend
 mode tcp
 bind 192.168.10.6:80 name OPT_http
 bind 192.168.10.6:135 name dcom
 bind 192.168.10.6:443 name https
 bind 192.168.10.6:444 name https
 bind 192.168.10.6:448 name OPT_call_admission_control
 bind 192.168.10.6:4443 name web_services
 bind 192.168.10.6:5060 name OPT_sip_unsecured
 bind 192.168.10.6:5061 name sip_tls
 bind 192.168.10.6:5065 name app_sharing
 bind 192.168.10.6:5069 name qoe
 bind 192.168.10.6:5070 name OPT_med_fe_communication
 bind 192.168.10.6:5071 name OPT_sip_response_groups
 bind 192.168.10.6:5072 name OPT_sip_conference_attendant
 bind 192.168.10.6:5073 name OPT_sip_conference_announcement
 bind 192.168.10.6:5074 name OPT_sip_voice_control
 bind 192.168.10.6:5075 name OPT_incoming_sip_request
 bind 192.168.10.6:5076 name OPT_dialin_conferencing
 bind 192.168.10.6:5080 name OPT_call_admission
 bind 192.168.10.6:8080 name OPT_web_services
 option tcp-smart-accept
 timeout client 1800s
 default_backend bk_LYNC2010_INT_frontend

backend bk_LYNC2010_INT_frontend
 mode    tcp
 option tcp-smart-connect
 timeout connect 5s
 timeout server 1800s
 retries 3
 stick-table type ip size 10k expire 1h peers aloha
 stick on src
 balance leastconn
 default-server inter 5s fall 3 rise 2 on-marked-down shutdown-sessions
 server 2010lyfe1 192.168.10.31 weight 10 check observe layer4 port 5061 check-ssl
 server 2010lyfe2 192.168.10.32 weight 10 check observe layer4 port 5061 check-ssl
```

5 SSL Offloading, SSL bridging

For some configuration templates provided in this guide, you may need to host your Lync certificates into the **ALOHA load-balancer**.
Documentation to configure SSL offloading and SSL bridging is available from **Exceliance** website: Resources > FAQ and Technical articles, then download the following PDF:

- AN-0021-EN - Implementation of a SSL frontend
- AN-0022-EN - Implementation of a backend SSL
- AN-0023-EN - Managing SSL backend & frontend
- AN-0024-EN - Managing SSL chained certificates

6 Going further with the ALOHA Load-Balancer

As mentioned in introduction, bear in mind that most services can be load-balanced via DNS, thanks to the smart Lync 2010 client protocol.
There are many topologies available for a **Lync 2010** infrastructure and the **ALOHA Load-balancer** can be used in any of them.
Purpose of this document is to provide the main line of configuring the **ALOHA load-balancer** for **Lync 2010**. The features below can be done with the ALOHA Load-Balancer, but are not explained in this documentation. Please contact Exceliance Pre-sales team or your Exceliance partner for help and information.

- DDOS protection on external Edge services
- Advanced health checking on TCP based services
- Application level health check on web Services

7 Contact Us

Email: contact@exceliance.fr

Website: `http://www.exceliance.fr/en`

Blog: `http://blog.exceliance.fr/`