



■ **Deployment Guide**

# AX Series for Microsoft Lync Server 2010



## TABLE OF CONTENTS

Introduction.....	3
Deployment Guide Overview.....	5
Deployment Prerequisites and Assumptions.....	7
AX Deployment for Lync Server 2010 Roles.....	7
AX Series Load Balancer .....	8
Logging onto the CLI .....	8
Logging onto the AX Graphical User Interface.....	10
Configuration Requirement Tables .....	11
Feature Templates and Configuration.....	14
A. How To Create a TCP Idle Timeout Template.....	14
B. How To Create Persistence with a Source-IP Persistence Template.....	16
C. How To Configure Source NAT.....	17
Feature Configuration.....	18
A. How To Configure SIP Monitoring for the Front End Server .....	18
Load Balancing Enterprise Pool for Front End Servers .....	20
Load Balancing Enterprise Pool for Internal Edge Servers .....	27
Load Balancing Enterprise Pool for External Edge Servers .....	34
Summary and Conclusion .....	41

## INTRODUCTION

The AX Series of Application Delivery Controllers (ADCs) provide advanced load balancing services for Microsoft Lync 2010. AX hardware-based models as well as the software-based model (SoftAX) are certified by Microsoft for Lync deployment:

<http://technet.microsoft.com/en-us/lync/gg269419>

Microsoft Lync 2010 Server was released on November 2010 as the successor to Microsoft Office Communicator 2007 R2, commonly known as OCS. Microsoft Lync is the next-generation unified communications platform that delivers accessibility among different Microsoft Office Applications such as Microsoft Outlook, Microsoft Word, and Microsoft SharePoint. A10 Networks' partnership with Microsoft provides a scalable, efficient and secure solution geared for the enterprise marketplace.

### **Microsoft Lync 2010 Server Advantages:**

- Unified Management platform and single management infrastructure.
- Rich client application that provides presence, instant messaging (IM), voice, ad hoc collaboration (desktop sharing) and online meeting capabilities through a single interface.
- Lync 2010 is easy to use, works closely with familiar tools such as SharePoint and Office applications, and drives user adoption with powerful features and a streamlined communications experience.
- Client dashboard shows common functions such as dial pad, visual voicemail, contact list, and active conversations.
- Ushers in a new connected user experience transforming every communication into an interaction that is more collaborative, engaging, and accessible from anywhere either from internal or external users.
- Microsoft Lync Server 2010 answers users' needs for communications tools that make their work easier and are available anywhere, anytime—including within the context of other applications.
- The users get an experience that is consistent and familiar across PC, phone, and browser.

For more information on Microsoft Lync 2010 Server, visit:

<http://lync.microsoft.com/en-us/Pages/default.aspx>

**Other Useful Links:**

Microsoft Lync Hardware and Software Requirements

<http://technet.microsoft.com/en-us/library/gg398438.aspx>

Reference Architecture: Scaled Consolidated Edge (Hardware Load Balanced)

<http://technet.microsoft.com/en-us/library/gg398478.aspx>

Reference Architecture: Port Summary for Scaled Consolidated Edge (Hardware Load Balanced)

<http://technet.microsoft.com/en-us/library/gg398739.aspx>

Ports and Protocols for Internal Servers

<http://technet.microsoft.com/en-us/library/gg398833.aspx>

**Benefits of A10 Networks AX Series Application Delivery Controller:**

- **Scalability** – Enterprises can provide Lync services to a very high number of employees, load balancing each client to the most optimal of the Lync servers at any given point in time.
- **High Availability** – Lync services provide guaranteed uptime even if a Lync Server goes offline or a Lync Server goes into maintenance mode.
- **Performance** – End-users access their Lync application faster thanks to multiple Lync server optimizations such as, but not limited to, compression and SSL offload.
- **Security** – Services are protected from malicious traffic such as DDoS attacks and other attacks.
- **Flexibility** – All Lync server accessibility to IM, Conferencing, Desktop Sharing, Presence, and Voice is optimized with a transparent load balancer.

## DEPLOYMENT GUIDE OVERVIEW

This deployment guide contains step-by-step configuration procedures for the A10 Networks AX Series Application Delivery Controllers (ADCs) to support the Microsoft Lync 2010 Enterprise Server solution. This deployment guide has been tested specifically for Microsoft Lync 2010 Enterprise Server Edition. This deployment guide does not apply to Microsoft OCS 2007 deployments. For the AX Series Microsoft OCS Deployment Guide please visit [www.a10networks.com](http://www.a10networks.com).

The lab topology (Figure 1) below is designed to support internal and external users with high availability voice, IM, desktop sharing and conferencing communications. The lab topology is deployed with two servers in each application pool and the topology can have additional servers if needed. For a server to be added, it must have the same server role configuration as the other servers in the application pool.

The lab topology was deployed with three A10 Networks AX devices to support different network segments within the deployment. The three segments are internal, internal edge and external edge. The segments are highlighted in the lab topology below.

## Topology Setup

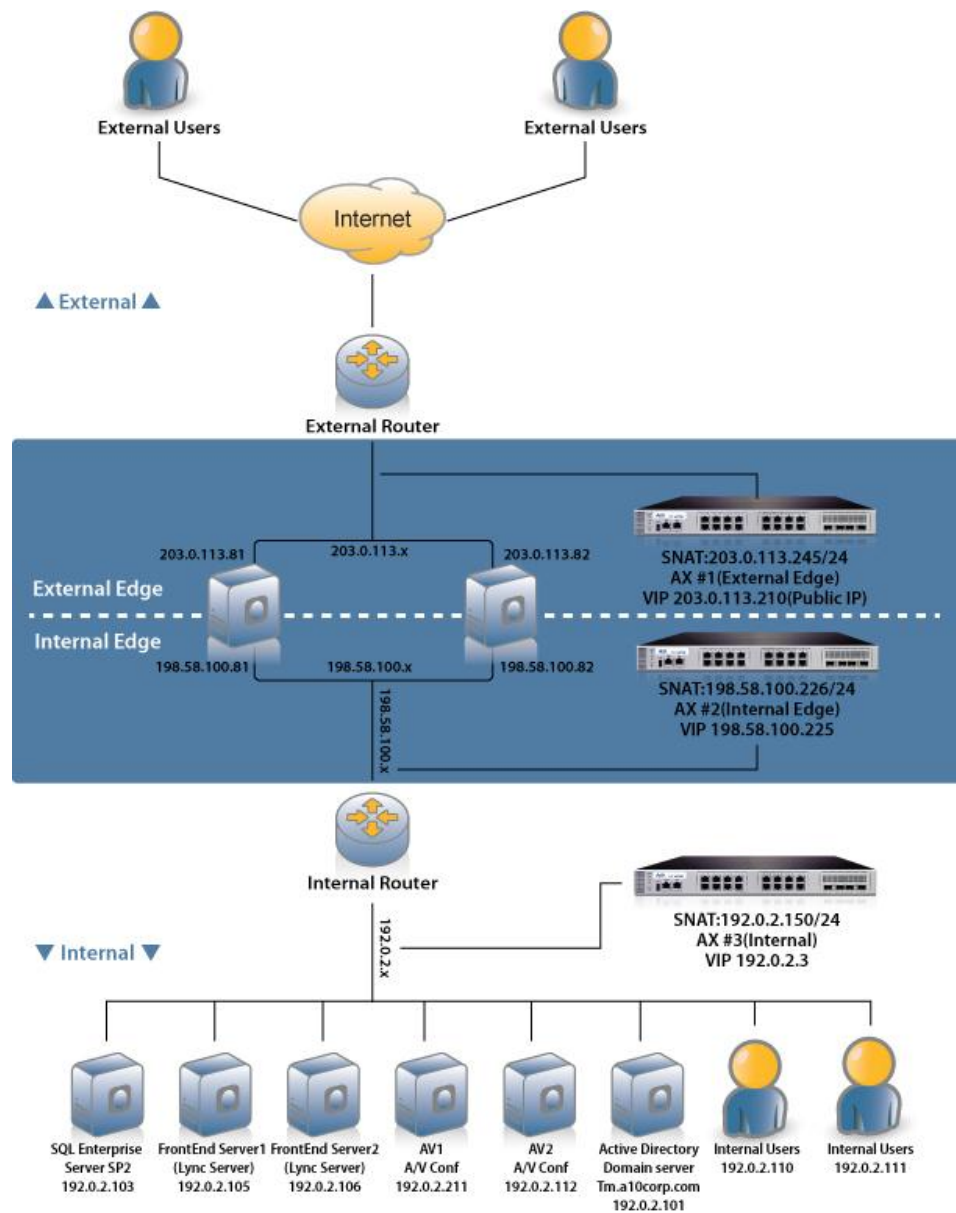


Figure 1: Lab Topology

## DEPLOYMENT PREREQUISITES AND ASSUMPTIONS

The deployment guide testing was based on the following configuration:

- A10 Networks AX Series appliances running version 2.6. Other versions of the AX Series also support Lync 2010.
- The Microsoft Lync 2010 Server was tested on Voice, Instant Messaging (IM), Presence, Desktop Collaboration and Audio Visual (AV) conferencing applications. Testing was performed for both internal and external users.
- Testing was performed using Microsoft Lync Server 2010 Enterprise Server with the 64-bit Microsoft SQL Server Enterprise Edition Version 10.0.4000.0.
- All Lync 2010 Server Components were running on Windows 2008 (64-bit) Standard Edition Server Operating System.
- Lync Clients were running Windows 7 Operating System.
- The lab setup was based on One-Arm deployment.

## AX DEPLOYMENT FOR LYNC SERVER 2010 ROLES

The Lync server solution has multiple servers within the solution. The server roles are described below.

**Front End Server (Lync Servers)** – The front end servers provide user authentication, registration, presence, IM, web conferencing and application sharing functionality. Front end servers also provide address book service and distribution list expansion. Front end servers are provisioned in a front end pool and configured identically to provide scalability and failover capability to Lync users.

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

**Back End Server** – The back end servers are Microsoft SQL servers that 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 single back end server; however, a cluster of two or more servers is recommended for failover.

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

**AV Conferencing Server** – Provides Audio Video conferencing functionality to the Lync solution. The AV server can be deployed as a single server or as a pool of servers for redundancy.

## AX SERIES LOAD BALANCER

AX Series devices provide the following management interfaces:

- Command-Line Interface (CLI) – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)
- Graphical User Interface (GUI) – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

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

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

## LOGGING ONTO THE CLI

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

*Note: The default IP Address of the AX device is 172.31.31.31.*



To log onto the CLI using SSH:

1. On a PC connected to a network that can access the AX device's management interface, open an SSH connection to the IP address of the management interface.
2. Generally, if this is the first time the SSH client has accessed the AX device, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. (Press "**Enter**".)
3. At the "login as:" prompt, enter the admin username.
4. At the Password: prompt, enter the admin password. If the admin username and password are valid, the command prompt for the User EXEC level of the CLI appears:

```
AX>
```

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

*Note: The "AX" in the CLI prompt is the hostname configured on the device, which is "AX" by default. If the hostname has already been changed, the new hostname appears in the prompt instead of "AX".*

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. (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:

```
AX#
```

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

```
AX(config)#
```

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

## LOGGING ONTO THE AX GRAPHICAL USER INTERFACE

To log onto the GUI:

1. In your web browser, navigate to the management IP address of the AX device.

A login dialog is displayed. The name and appearance of the dialog depend on the browser you are using.

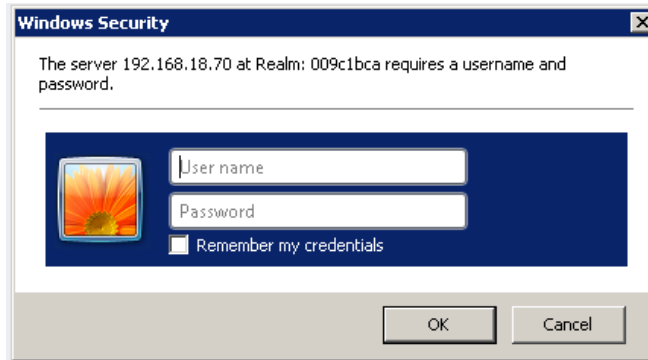


Figure 2: GUI Login Dialog

*Note: The default admin credentials are Username: "admin" and Password: "a10".*

2. Enter your admin **Username** and **Password** and click "**OK**".

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

## CONFIGURATION REQUIREMENT TABLES

The following tables list the services required for Lync 2010 Enterprise Server deployment.

Table 1: Internal Front End Services					
Server Role	Port	VIP TYPE	Source NAT	Feature Templates	Usage Notes
Lync Front End Servers	135	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Used for DCOM-based operations such as moving users, user replicator synchronization, and address book synchronization.
Lync Front End Servers	443	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for communication from front end servers to the web farm FQDNs (the URLs used by IIS web components).
Lync Front End Servers	444	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for communication between Lync Server components that manage the conference state and the individual servers.
Lync Front End Servers	5061	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Front end pools for all internal SIP communications between servers (MTLS), for SIP communication between server and client (TLS) and for SIP communication between front end servers and Mediation Servers (MTLS).

Table 2: Optional Internal Front End Services					
Server Role	Port	VIP TYPE	Source NAT	Feature Templates	Usage Notes
Lync Front End Servers	5060	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port used for front end servers for static routes to trusted services.
Lync Front End Servers	5065	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for incoming SIP requests for application sharing.
Lync Front End Servers	5071	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for incoming SIP requests for the response group application.
Lync Front End Servers	5072	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for incoming SIP requests for Microsoft Lync 2010 attendant (dial-in conferencing).
Lync Front End Servers	5073	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for incoming SIP requests for Lync Server conferencing announcement service.
Lync Front End Servers	5075	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for incoming SIP requests for the call park application.

Table 3: Services for Internal Edge					
Server Role	Port	VIP TYPE	Source NAT	Feature Templates	Usage Notes
Internal Edge Server	443	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for communication between the internal edge server farm FQDN used by Web Components.
Internal Edge Server	3478	UDP	Yes	<b>Health Monitor:</b> Default	Preferred path for media transfer between internal and external users (UDP).
Internal Edge Server	5061	TCP/TLS	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Used for external ports for SIP/MTLS communication for remote user access or federation.
Internal Edge Server	5062	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Used for authentication of AV users.
Internal Edge Server	8057	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for outgoing PSOM traffic sent to the web conferencing server.

Table 4: Services for External Edge					
Server Role	Port	VIP TYPE	Source NAT	Feature Templates	Usage Notes
External Edge-Access	443	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge-Access	5061	TCP	Yes	<b>Persistence:</b> Source-IP <b>TCP Idle Timeout:</b> 1200 <b>Health Monitor:</b> Default	Port for external SIP/MTLS communication for remote user access and federation.
External Edge-WebConf	443	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge-AV	443	TCP	Yes	<b>Persistence:</b> Source-IP <b>Health Monitor:</b> Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge-AV	3478	UDP	Yes	<b>Health Monitor:</b> Default	Used for external ports for STUN/UDP inbound and outbound media resources.

*Note: During feature selection (Figure 3) of the external edge pool install, you will be asked to deploy the Lync edge server pool with either a single or multiple FQDNs and IP addresses. Unselecting the “use a single FQDN and IP address” option will enable the external edge pool to have multiple IP configurations. The AX 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.*

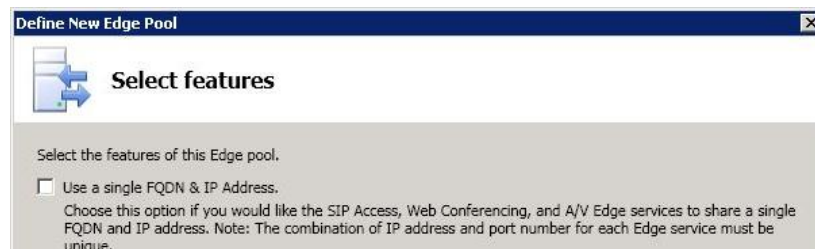


Figure 3: External Edge Pool Server Feature Selection

## Protocol Definitions

- STUN – Session Traversal Utilities for NAT (STUN)
- SIP – Session Initiation Protocol
- MTLS – Multiplexed Transport Layer Security
- PSOM – Persistent Shared Object Protocol
- TLS – Transport Layer Security
- FQDN – Fully Qualified Domain Name
- DCOM – Distributed Component Object Model

## FEATURE TEMPLATES AND CONFIGURATION

The following templates and configuration are required for each AX device.

- TCP Idle Timeout
- Source-IP Persistence
- Source Network Address Translation (NAT)

### A. HOW TO CREATE A TCP IDLE TIMEOUT TEMPLATE

- Navigate to **Config > Service > Template > L4 > TCP**.

Template >> L4 >> TCP >> Create

TCP		
Name: *	<input type="text" value="TCP IDLE 1200"/>	
Idle Timeout:	<input type="text" value="1200"/>	Seconds
Force Delete Timeout:	<input type="text"/>	Seconds
Initial Window Size:	<input type="text"/>	
Reset Forward:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Reset Receive:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

OK  Cancel

Figure 4: L4 TCP Template

*Note: The TCP idle timeout of 1200 seconds is the idle time required before a TCP connection is reset within the AX device.*

2. Click **“Add”** and name the template as: **“TCP IDLE 1200”**
3. Enter the following required parameters:
  - Idle Timeout: **1200 Seconds**
  - **“Enable”** Reset Forward – sends a TCP RST to the real server after a session times out
  - **“Enable”** Reset Receive – sends a TCP RST to the client after a session times out
4. Once completed, click **“OK”** and **“Save”** the configuration.
5. Repeat the above steps for each AX device.

## B. HOW TO CREATE PERSISTENCE WITH A SOURCE-IP PERSISTENCE TEMPLATE

1. Navigate to **Config Mode > Service > Template> Persistence**.

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

Source IP Persistence	
Name: *	Source IP Persistence
Match Type:	Server <input type="checkbox"/> Scan All Members
Timeout:	1200 Minutes
Don't Honor Conn Rules:	<input type="checkbox"/>
Netmask:	255.255.255.255

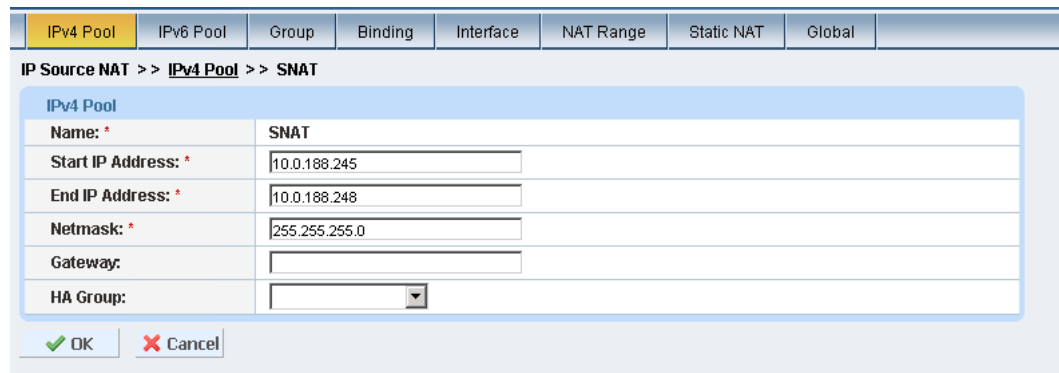
Figure 5: Source-IP Persistence Template

2. Select **"Source IP Persistence"** from the drop-down list.
3. Click **"Add"** and name the template as: **"Source IP Persistence"**.
4. Enter the following required parameters:
  - **Match Type: Server**
  - **Timeout: 1200 Minutes**
  - **Netmask: 255.255.255.255 (Default)**
5. Click **"OK"** and **"Save"** the configuration.
6. Repeat the above steps for each AX device.



## C. HOW TO CONFIGURE SOURCE NAT

1. Navigate to **Config > Service > IP Source NAT > IP V4 Pool**.
2. Click “**Add**” and enter the following required parameters:
  - Name: “**SNAT**”
  - Start IP Address: *10.0.188.245*
  - End IP Address: *10.0.188.248*
  - Netmask: *255.255.255.0*



The screenshot shows a configuration window for IP Source NAT. The breadcrumb path is "IP Source NAT >> IPv4 Pool >> SNAT". The configuration table is as follows:

IPv4 Pool	
Name: *	SNAT
Start IP Address: *	10.0.188.245
End IP Address: *	10.0.188.248
Netmask: *	255.255.255.0
Gateway:	
HA Group:	

At the bottom of the form, there are two buttons: "OK" (with a green checkmark icon) and "Cancel" (with a red X icon).

Figure 6: IPv4 Pool Source NAT

3. Click “**OK**” and “**Save**” the configuration.

*Note: For One-Arm deployments, Source NAT (SNAT) must use the same subnet as the Lync server host.*

## FEATURE CONFIGURATION

The following configuration is required for SIP Monitoring for Front End servers.

### A. HOW TO CONFIGURE SIP MONITORING FOR THE FRONT END SERVER

This setting can be enabled from the Lync 2010 Topology Builder under Enterprise Edition Front End Pools. The purpose of this feature is to enable the AX device to monitor the state of the pool servers via port 5060.

1. Launch “**Lync Server Topology Builder**” from one of the Microsoft front end servers.
2. Select “**Download Topology**” from existing deployment and save the configuration.
3. Select “**Enterprise Edition Front End Pool**” name.
4. Edit the pool name properties. Select “**Enable hardware load balancer monitoring port**”, enter “**5060**” and Click “**OK**”.

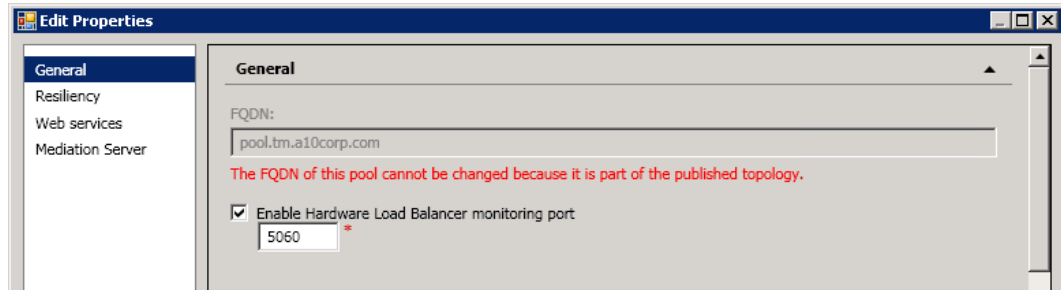


Figure 7: Microsoft Lync Edit General Properties

5. Right-click the topology name “A10 Lab”, select **Topology** and **Publish**.

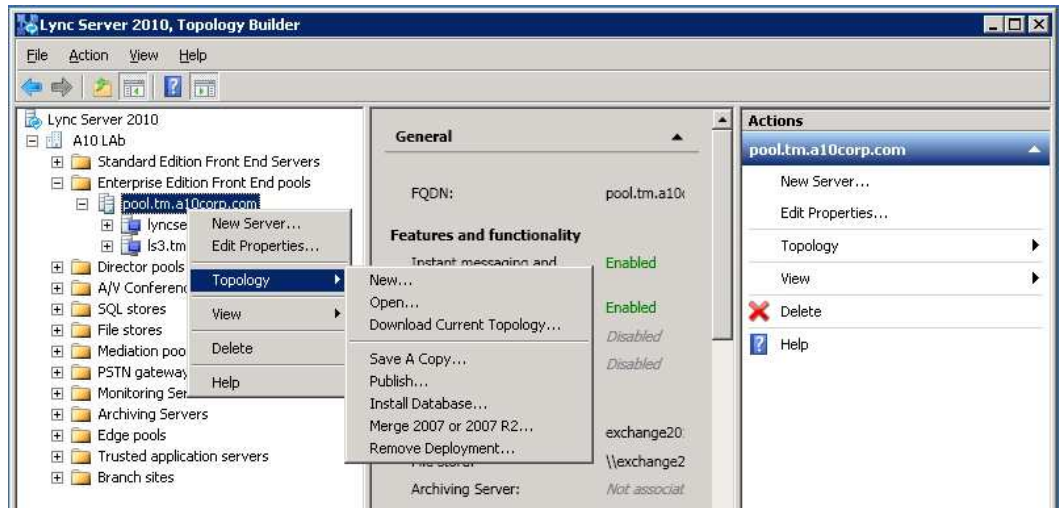


Figure 8: Microsoft Lync Topology Builder

*Note: Any changes within the topology must be “**Published**” for the changes to take effect.*

## LOAD BALANCING ENTERPRISE POOL FOR FRONT END SERVERS

A site can consist of one or more pools, each containing one or more Lync servers. Within each pool dedicated services run, such as AV conferencing, IM (front end) and IM/presence/collaboration. A front end server pool is a collection of Lync servers that will process basic IM, presence and collaboration requests. All servers in a pool must run exactly the same service, so that failure of a server within a pool does not disturb the pool.

### Lab Setup: Front End Servers

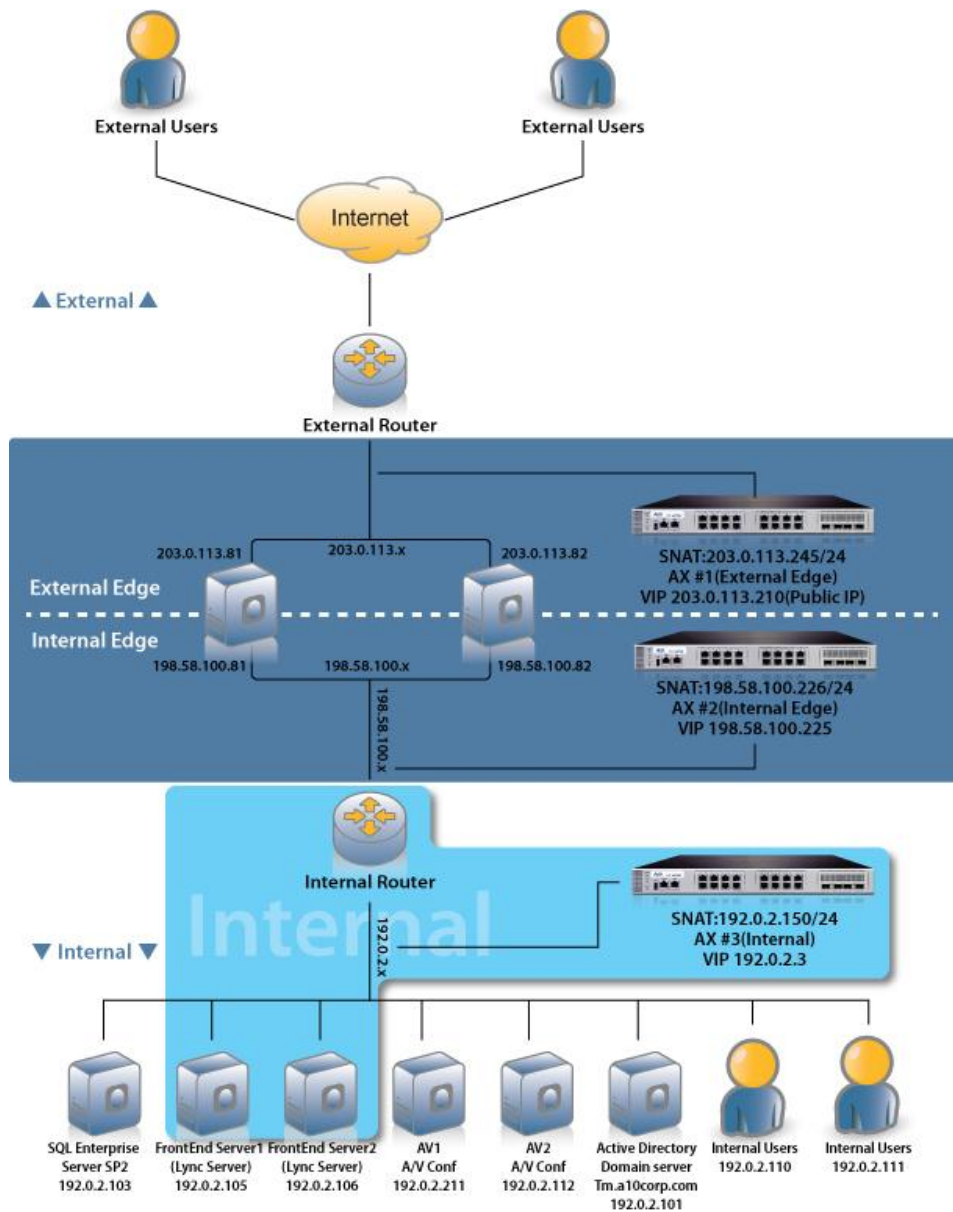


Figure 9: Front End Server Topology

To configure a load balanced Lync Front End Enterprise pool within the AX device:

- A. Add the servers.
- B. Add the servers to a service group.
- C. Bind the service group to a virtual server.

#### A. To Add the Servers

1. Navigate to **Config > Service > SLB > Server**.
2. Click **“Add”** to add a new server.
3. Within the Server section, enter the following required information:
  - Name: **“LS1”**
  - IP Address/Host: **192.0.2.105**

SLB >> Server >> Create

General	
Name: *	LS1
IP Address/Host: *	192.0.2.105 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default) ▼
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	
Slow Start:	<input type="checkbox"/>
Spoofing Cache:	<input type="checkbox"/>
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Template:	default ▼
Description:	

Figure 10: Real Server Configuration

4. To add ports to the server configuration, navigate to **Config > Service > SLB > Server**.
5. Click **“Add”** to add ports.

- Enter **Port**, **Protocol** type and click “**Add**”.

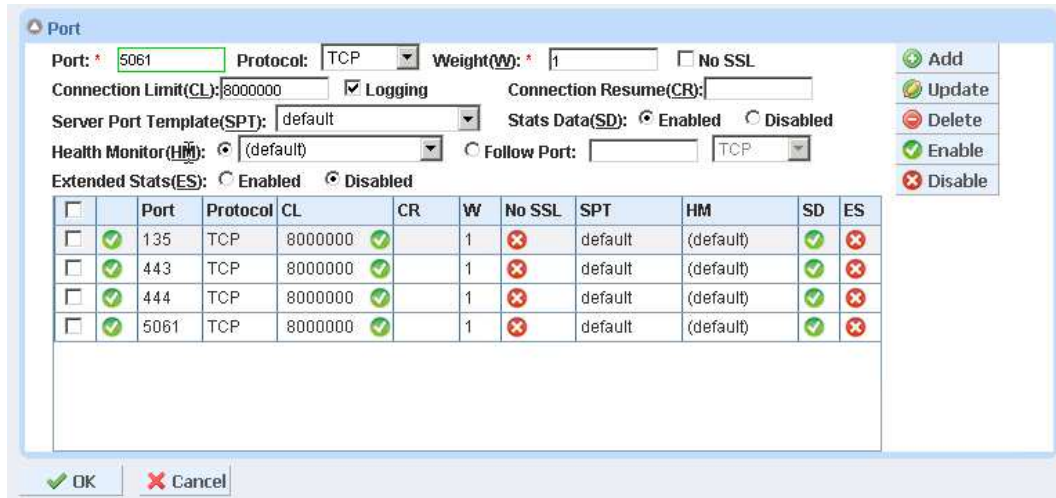


Figure 11: Server Port Configuration

Note: Refer to **Table 1: Internal Front End Services** for required ports. For optional services for Internal Front End refer to **Table 2: Optional Services for Internal Front End**.

- Click “**OK**” and “**Save**” the configuration.

## B. To Add the Servers to a Service Group

1. Navigate to **Config > Service > SLB > Service Group**.
2. Click **Add** to add a new Service Group called “**SG443**”.
3. In the Service Group section, enter the following information.
  - Name: “**SG135**”
  - Type: **TCP**
  - Algorithm: **Least Connection**

SLB >> **Service Group** >> Create

Service Group	
Name: *	SG135
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	Default
Min Active Members:	<input type="checkbox"/>
<input type="checkbox"/>	Send client reset when server selection fails
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	

Figure 12: Service Group Configuration

4. Add at least one or more servers from the server drop-down list, each with a port. In **Figure 13**, the server names **LS1** and **LS2** are entered, each with port **135**.

Server

IPv4/IPv6:  IPv4  IPv6

Server: \*  Port: \*

Server Port Template(SPT): default Priority: 1

Stats Data:  Enabled  Disabled

<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data
<input checked="" type="checkbox"/>	LS2	135	default	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	LS1	135	default	1	<input checked="" type="checkbox"/>

OK  Cancel

Figure 13: Service Group Configuration

Note: Complete the same steps above to configure the service group for ports 443, 444 and 5061.

### C. To Bind the Service Group to a Virtual Server

1. Navigate to **Config > Service > SLB > Virtual Server**.
2. Click **“Add”** to add a Virtual Server.
3. Enter the following information:
  - Name: **“Internal Front End VIP”**
  - IP Address: *192.0.2.3*

SLB >> Virtual Server >> Create

General	
Name: *	Internal Front End VIP <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	192.0.2.3 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
When-All-Ports-Down:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Group:	<input type="text"/>
Virtual Server Template:	default
PBSLB Policy Template:	<input type="text"/>
Description:	<input type="text"/>

Figure 14: Virtual Server Configuration

4. Click **“Add”** under the Port Section.
5. Add the required virtual server ports.



6. Click “Add” to add Ports:

- Type: **TCP**
- Port: “**443**”
- Service Group: “**SG443**”

SLB >> Virtual Server >> Internal Front End VIP >> Port >> Create

Virtual Server Port	
Virtual Server:	Internal Front End VIP
Type: *	TCP
Port: *	443
Service Group:	SG443
Connection Limit:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input checked="" type="radio"/> Reset <input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
<input type="checkbox"/>	Send client reset when server selection fails
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Connection Mirror:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Direct Server Return:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SYN Cookie:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Source NAT traffic against VIP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	

Figure 15: Internal Edge VIP Configuration

Note: Requirements for service templates such as Source NAT Pool, TCP-Proxy and Persistence are defined in the Configuration Requirements Table. Refer to [Table 1: Internal Front End Services](#).

Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	SNAT
aFlex:	<input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	
PBSLB Policy Template:	

Figure 16: Feature Templates

7. Click **OK** and **Save** the configuration.

*Note: Complete the same steps above for the virtual service ports required for Internal Front End Enterprise Services.*

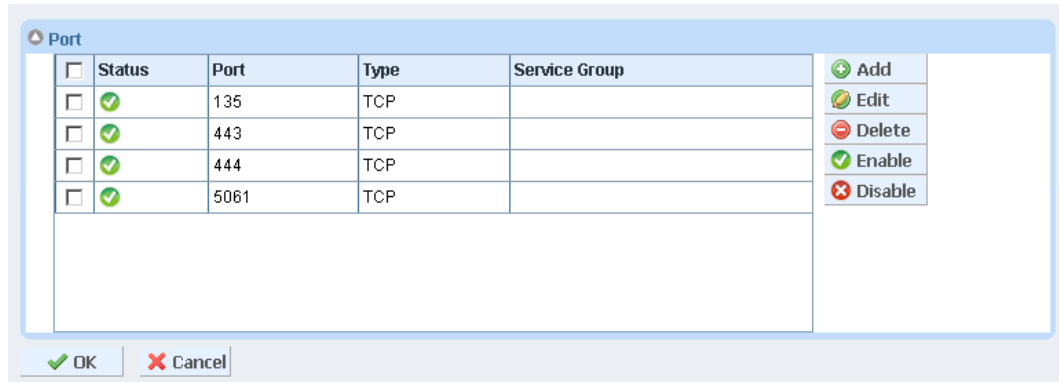


Figure 17: Virtual Server Port Configuration

## LOAD BALANCING ENTERPRISE POOL FOR INTERNAL EDGE SERVERS

### Lab Setup: Internal Edge

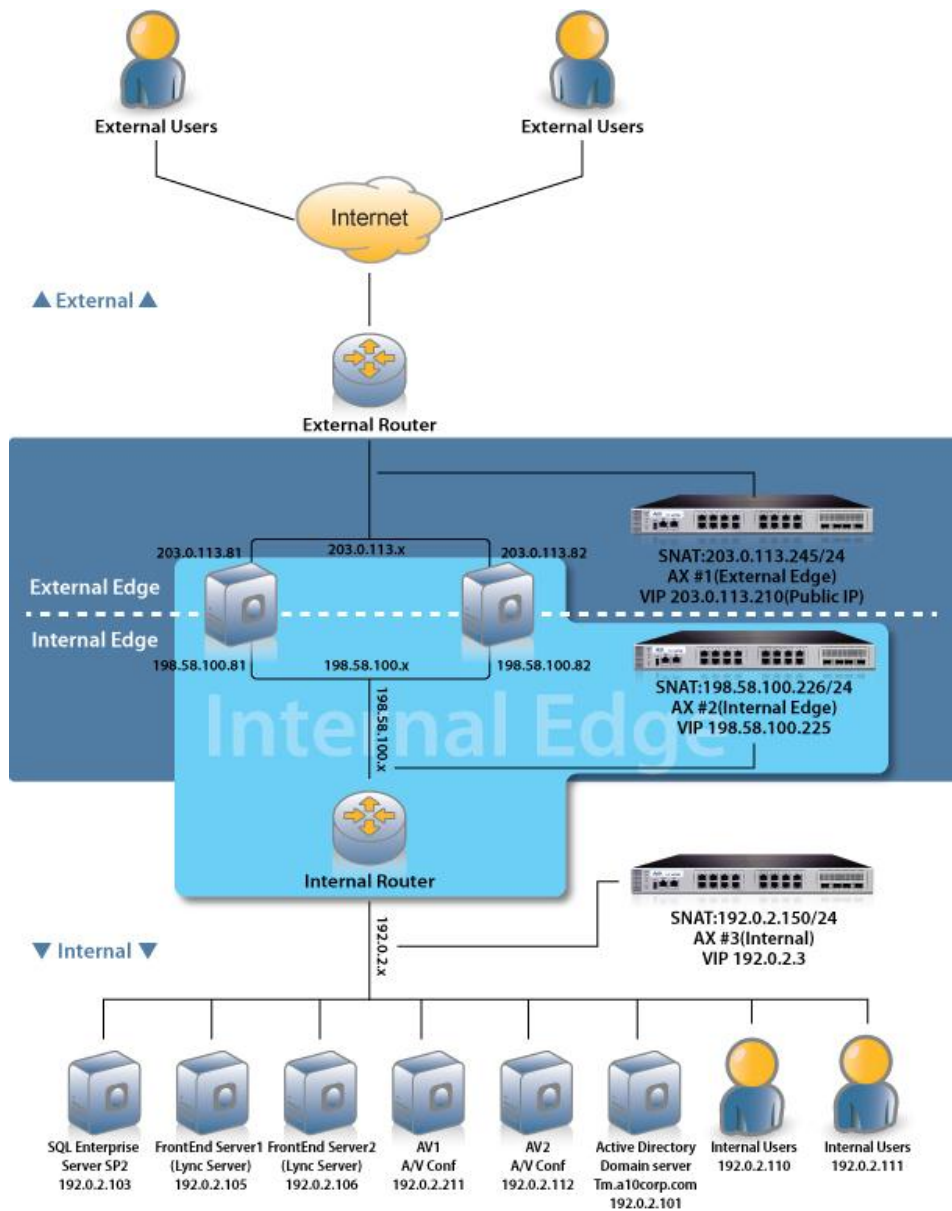


Figure 18: Internal Edge Topology

To configure a load balanced Lync Internal Edge Server within the AX device:

- A. Add the servers.
- B. Add the servers to a service group.
- C. Bind the service group to a virtual server.

#### A. To Add the Servers

1. Navigate to **Config > Service > SLB > Server**.
2. Click **“Add”** to add a new Server.
3. Within the Server Menu enter the following required information:
  - Name: **“Internal Edge Server 1”**
  - IP Address/Host: *198.58.100.81*

SLB >> Server >> Create

General	
Name: *	Internal Edge Server 1
IP Address/Host: *	198.58.100.81 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default) ▼
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	
Slow Start:	<input type="checkbox"/>
Spoofing Cache:	<input type="checkbox"/>
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Template:	default ▼
Description:	

Figure 19: Internal Edge Server Configuration

4. Select **"Add"** under Port.
5. Add the Virtual Server Ports and Protocol types shown in the following figure:

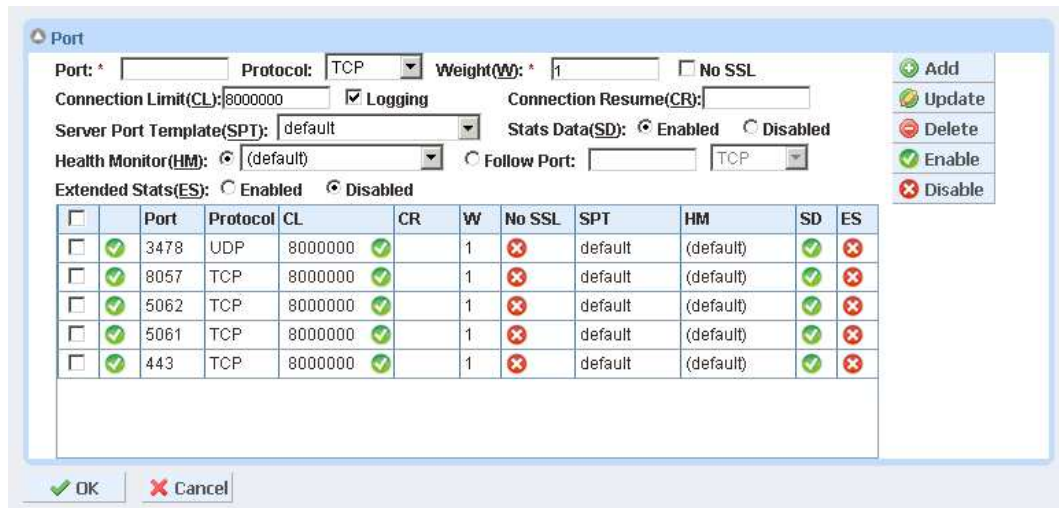


Figure 20: Server Port Configuration

Note: Refer to [Table 3: Services for Internal Edge](#) for required ports for Internal Edge Services.

## B. To Add the Servers to a Service Group

1. Navigate to **Config > Service > SLB > Service Group**.
2. Click **“Add”** to add a new Service Group called **“SG443”**
3. Within the Service Group Menu enter the following Information:
  - Name: **“SG443”**
  - Type: **TCP**
  - Algorithm: **Least Connection**

SLB >> **Service Group** >> Create

Service Group	
Name: *	SG443
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	Default
Min Active Members:	<input type="checkbox"/>
<input type="checkbox"/>	Send client reset when server selection fails
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	

Figure 21: Service Group Configuration

4. Add one or more servers from the server drop-down list, each with a port. In **Figure 22**, the server names **EdgeServerInternal1** and **EdgeServerInternal2** are entered, with port **443**.

The screenshot shows the 'Server' configuration window. At the top, there are radio buttons for 'IPv4' (selected) and 'IPv6'. Below that are fields for 'Server: \*' (a dropdown menu), 'Port: \*' (a text box), 'Server Port Template(SPT):' (a dropdown menu set to 'default'), and 'Priority:' (a dropdown menu set to '1'). There are also radio buttons for 'Stats Data:' with 'Enabled' selected. On the right side, there is a vertical stack of buttons: '+ Add', 'Update', '- Delete', 'Enable', and 'Disable'. At the bottom, there are 'OK' and 'Cancel' buttons.

<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data
<input checked="" type="checkbox"/>	EdgeServerInternal2	443	default	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	EdgeServerInternal1	443	default	1	<input checked="" type="checkbox"/>

Figure 22: Service Group Server Lists

*Note: Complete the same steps above for the service group for Internal Edge Services. Refer to [Table 3: Services for Internal Edge](#).*

### C. To Bind the Service Group to a Virtual Server

1. Navigate to **Config > Service > SLB > Select Virtual Server**.
2. Click the **"Add"**.
3. Enter the following configuration information:
  - Name: **"Internal Edge VIP"**
  - IP Address: *198.58.100.225*

4. Add the virtual server ports with the corresponding service-group name.

SLB >> **Virtual Server** >> Create

General	
Name: *	Internal Edge VIP <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	198.58.100.225 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
When-All-Ports-Down:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Group:	<input type="text"/>
Virtual Server Template:	default
PBSLB Policy Template:	<input type="text"/>
Description:	<input type="text"/>

Figure 23: Virtual Server Configuration

5. Click “**Add**” under the Port section.
6. Add the required virtual server ports:
  - Type: **TCP**
  - Port: “**443**”
  - Service Group: “**SG443**”

SLB >> **Virtual Server** >> **Internal Edge VIP** >> **Port** >> Create

Virtual Server Port	
Virtual Server:	Internal Edge VIP
Type: *	TCP
Port: *	443
Service Group:	SG443
Connection Limit:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input type="radio"/> Reset <input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
<input type="checkbox"/>	Send client reset when server selection fails
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Connection Mirror:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Direct Server Return:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SYN Cookie:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Source NAT traffic against VIP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Figure 24: Internal Edge Configuration



*Note: Requirements for service templates such as Source NAT Pool, TCP-Proxy and Persistence are defined in the Configuration Requirements Table. Refer to [Table 3: Services for Internal Edge](#).*

Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	SNAT
aFlex:	<input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	
PBSLB Policy Template:	

Figure 25: Feature Templates

7. Click “OK” and “Save” to save the configuration.

<input type="checkbox"/>	Status	Port	Type	Service Group	
<input type="checkbox"/>	✓	443	TCP	SG443	+
<input type="checkbox"/>	✓	3478	UDP	SG3478	+
<input type="checkbox"/>	✓	5061	TCP	SG5061	+
<input type="checkbox"/>	✓	5062	TCP	SG5062	+
<input type="checkbox"/>	✓	8057	TCP	SG8057	+

+ Add  
+ Edit  
- Delete  
✓ Enable  
✗ Disable

✓ OK ✗ Cancel

Figure 26: Virtual Server Port Configuration

*Note: Refer to [Table 3: Services for Internal Edge](#) for the ports required for Internal Edge Services.*

## LOAD BALANCING ENTERPRISE POOL FOR EXTERNAL EDGE SERVERS

The purpose of the Edge Server is to provide external users' access to the Lync server across a corporate firewall. The edge servers will be able to provide all features within Lync services including conferencing, remote user access, federation and public IM connectivity. The edge servers can be deployed in a single or multi-server deployment. A load balancer is necessary in multi-server deployment to provide redundancy and resiliency to the application.

### Lab Setup: External Edge

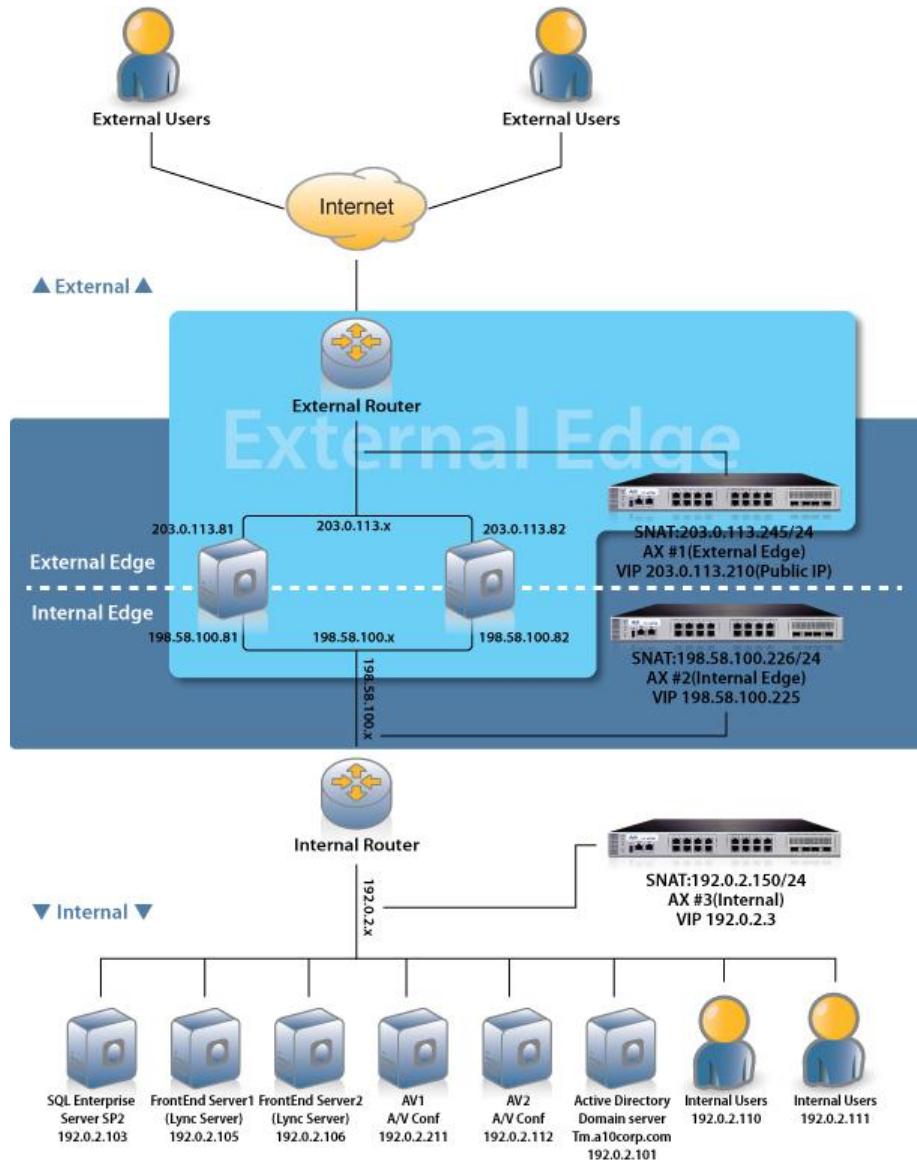


Figure 27: External Edge Topology

Note: The external edge topology above depicts a single FQDN and IP address configuration.

To configure a load balanced Lync External Edge Server within the AX device:

- A. Add the servers.
- B. Add the servers to a service group.
- C. Bind the service group to a virtual server.

#### A. To Add the Servers

1. Navigate to **Config > Service > SLB > Server**.
2. Click **“Add”** to add a new Server.
3. Within the Server Menu enter the following required information:
  - Name: **“External Edge Server 1”**
  - IP Address/Host: *203.0.113.81*

SLB >> Server >> Create

General	
Name: *	External Edge Server 1
IP Address/Host: *	203.0.113.81 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default) ▼
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	
Slow Start:	<input type="checkbox"/>
Spoofing Cache:	<input type="checkbox"/>
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Template:	default ▼
Description:	

Figure 28: Virtual Server Configuration

4. Click **“Add”** under the Port Section.
5. Add the virtual server ports shown in the following figure:

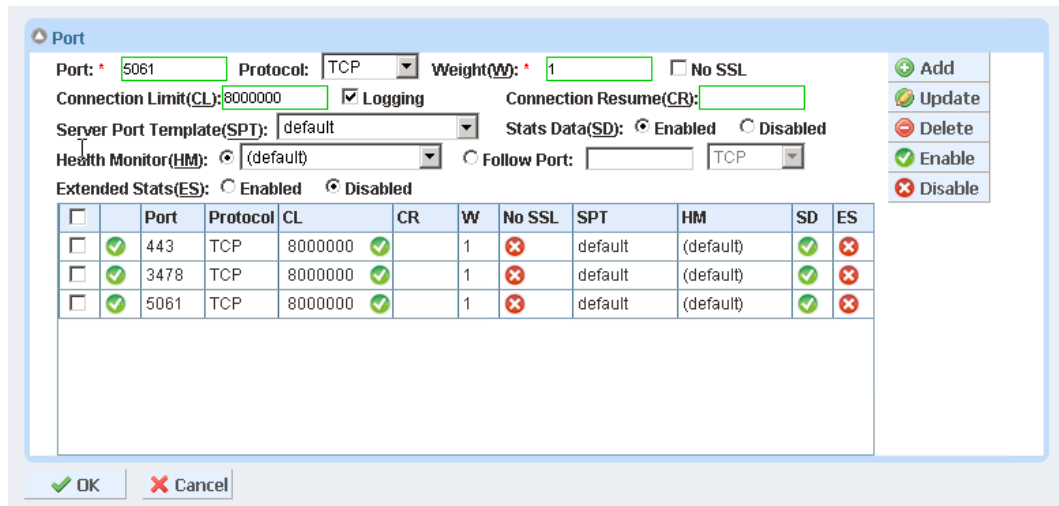


Figure 29: Virtual Server Ports

Note: Refer to [Table 4: Services for External Edge](#) for the ports required for External Edge Services.

#### B. To Add the Servers to a Service Group

1. Navigate to **Config > Service > SLB > Service Group**.
2. Click **“Add”** to add a new service group.

3. Within the Service Group Menu enter the following Information:
  - Name: **“SG443”**
  - Type: **TCP**
  - Algorithm: **Least Connection**

SLB >> **Service Group** >> Create

**Service Group**

Name: *	<input type="text" value="SG443"/>
Type:	<input type="text" value="TCP"/>
Algorithm:	<input type="text" value="Least Connection"/>
Health Monitor:	<input type="text" value="Default"/>
Min Active Members:	<input type="checkbox"/>
<input type="checkbox"/>	Send client reset when server selection fails
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	<input style="width: 100%;" type="text"/>

Figure 30: Service Group Configuration

4. Add one or more servers within the server drop-down list, with ports. In **Figure 31**, the server names **ExternalEdgeServer1** and **ExternalEdgeServer2** are entered, with port **443**.

**Server**

IPv4/IPv6:  IPv4  IPv6

Server: \*  Port: \*

Server Port Template(SPT):  Priority:

Stats Data:  Enabled  Disabled

<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data
<input checked="" type="checkbox"/>	ExternalEdgeServer2	443	default	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ExternalEdgeServer1	443	default	1	<input checked="" type="checkbox"/>

Figure 31: Service Group Server Lists

Note: Complete the same steps above for the service group for required for External Edge Services. Refer to [Table 4: Services for External Edge](#).

### C. To Bind the Service Group to a Virtual Server

1. Navigate to **Config > Service > SLB > Select Virtual Server**.
2. Click **“Add”**.
3. Enter the following configuration information:
  - Name: **“External Edge VIP”**
  - IP Address: *203.0.113.210*
4. Add the virtual server ports with the corresponding service-group name.

SLB >> **Virtual Server** >> Create

General	
Name: *	External Edge VIP <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	203.0.113.210 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
When-All-Ports-Down:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Group:	<input type="text"/>
Virtual Server Template:	default <input type="text"/>
PBSLB Policy Template:	<input type="text"/>
Description:	<input type="text"/>

Figure 32: Virtual Server Configuration

5. Click **“Add”** under the Port section.

6. Add the required virtual server ports, as shown in the following figures.

SLB >> Virtual Server >> External Edge VIP >> Port >> Create

Virtual Server Port	
Virtual Server:	External Edge VIP
Type: *	TCP
Port: *	443
Service Group:	SG443
Connection Limit:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input checked="" type="radio"/> Reset <input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
<input type="checkbox"/>	Send client reset when server selection fails
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HA Connection Mirror:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Direct Server Return:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SYN Cookie:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Source NAT traffic against VIP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Figure 33: Virtual Service Configuration

*Note: Requirements for service templates such as Source NAT Pool, TCP-Proxy and Persistence are defined in the Configuration Requirements Table. Refer to [Table 4: Services for External Edge](#).*

Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	SNAT
aFlex:	<input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	
PBSLB Policy Template:	

Figure 34: Virtual Service Templates

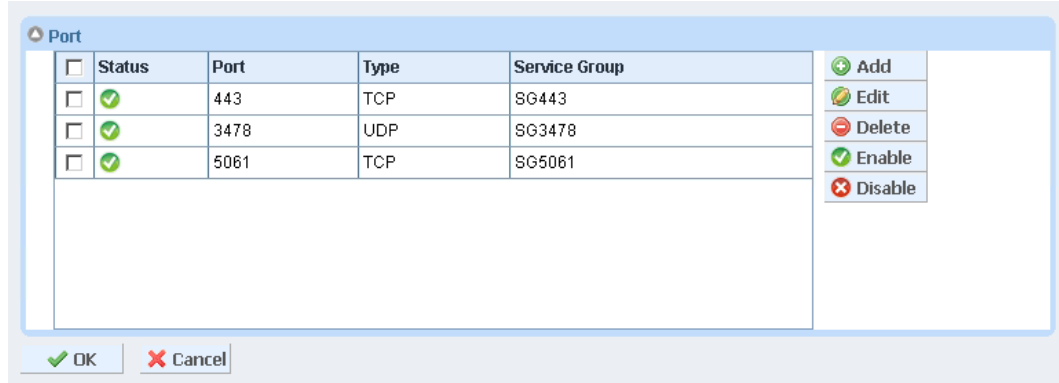


Figure 35: Virtual Server Ports

Note: Refer to [Table 4: Services for External Edge](#) for required ports for External Edge Services.

- Once completed, click “OK” and “Save” to save the configuration.



## SUMMARY AND CONCLUSION

The configuration steps described above show how to set up the AX for Microsoft Lync 2010 Server. By using the AX device to load balance Lync application services, the following key advantages are achieved:

- Transparent application load sharing.
- Higher availability when Lync Servers fail, so that there is no direct impact to how users access the applications.
- Higher utilization, as the AX device transparently load balances to multiple Lync Communication servers.
- Higher connection throughput and faster responsiveness experienced by end users, through offload of security processing to the AX device.

By using the AX Series Advanced Traffic Manager and Application Delivery Controller, significant benefits are achieved for all users of Microsoft Lync 2010 services.

For more information about AX Series products, refer to:

<http://a10networks.com/products/axseries.php>

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

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