Application Note

Ingate MEDIAtor

for

Microsoft Office Live Communications Server

Table of Content

Tested versions: Ingate SIParator version 4.4
Office Live Communications Server 2005[1], SP1
Office Communicator 2005 (1.0.559)

Revision History:

Revision	Date	Author	Comments
0.1	2006-06-16	Janne Magnusson	1st draft
1.0	2006-08-23	Janne Magnusson	Clean up and fixes
1.1	2006-11-27	Janne Magnusson	Added Firewall configuration

[1] LCS Standard Edition is tested for TLS and TCP while LCS Corporate Edition has only been tested using TCP and TLS.

1 Introduction

This is a technical description of how an Ingate MEDIAtor is configured together with a Microsoft Live Communication Server 2005.

The MEDIAtor sits alongside an LCS Access Proxy (AP) and relays media to and from remote and federated users. The MEDIAtor is made up of two parts. One is an Ingate SIParator with the LCS module installed. This is a physical piece of hardware that must be connected to the site's network. The other part is a Windows service that runs on a LCS Access Proxy.

2 Network Setup

The Ingate MEDIAtor provides great flexibility in the network configuration and you can first select the LCS architecture most suitable for your network and then choose the MEDIAtor configuration accordingly. For recommendations on the LCS architecture please see applicable documentation from Microsoft.

Figure 1 shows a typical Ingate MEDIAtor setup with the LCS and MEDIAtor located on the DMZ of the corporate firewall.

Requirements:

- The Ingate SIParator must have a public routable IP address on the external interface.
- Traffic between the SIParator and Internet must not be NATed
- Traffic between the SIParator and the internal LAN must not be NATed

Recommendations:

- To have different networks on the external and private side of the Access Proxy and SIParator.
- To have a dedicated network, ideally a cross cable, for communication between the SIParator and Access Proxy. This communication can use one any interface but it should be protected from the public Internet.
- To have a relay in the firewall that let the Access Proxy see the true IP address of the client. The functionality will be the same in any case but FENT in the Ingate module will then the used in all cases and it could possible consume more recourses.

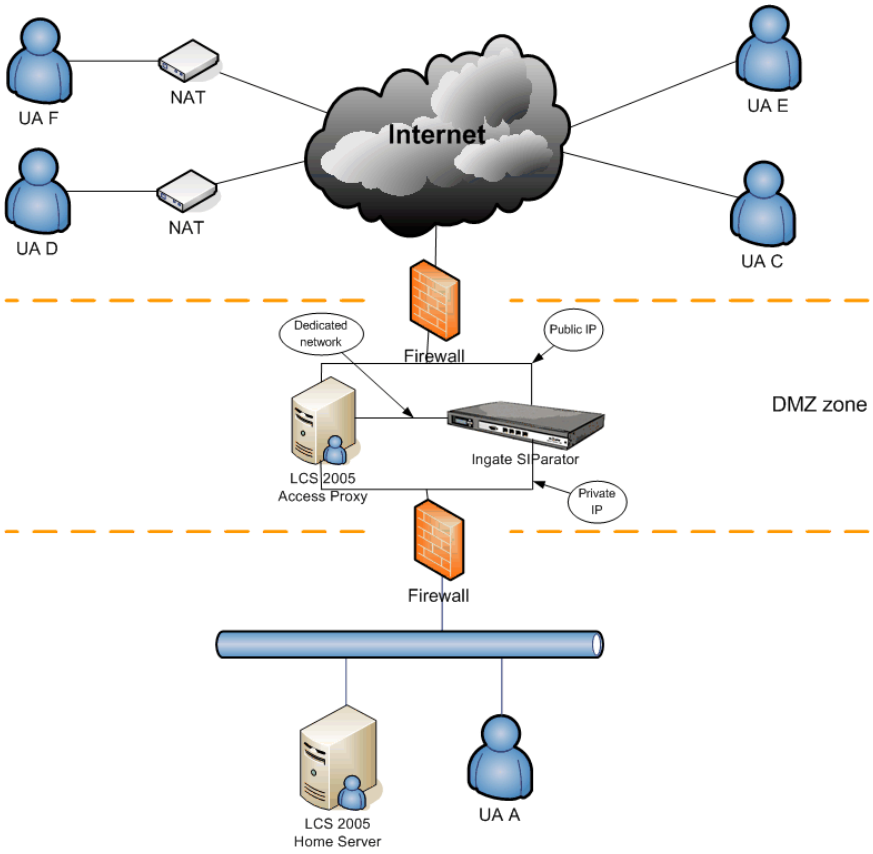


Figure 1

Alternative setups:

Figure 1 shows one typical setup but you may change this setup as long as the requirements mentioned above are followed. For example can the SIParator be configured in parallel with the existing firewall or with one interface on the DMZ and one on directly on the internal network. The SIParator and Access Proxy do not need to be located next to each other as shown in the picture, the only requirement is that they have a way to communicate directly to each other (preferably over a cross cable).

2.1 Firewall configuration

Configuration of the external firewall:

Traffic type	Transport	Src. IP	Dest. IP	Src. Port	Dst. Port
Voice/Video	UDP	MEDIAtor	Any	Media range*	All high
Voice/Video	UDP	Any	MEDIAtor	All High	Media range*
Application Sharing and File Transfer	TCP	MEDIAtor	Any	Media range*	All high
Application Sharing and File Transfer	TCP	Any	MEDIAtor	All High	Media range*

*) Media port range as configured on the MEDIAtor on the page SIP Service – Basic (default 58024-60999)

Configuration of the internal firewall:

Traffic type	Transport	Src. IP	Dest. IP	Src. Port	Dst. Port
Voice/Video	UDP	MEDIAtor	All Internal	Media range*	All high
Voice/Video	UDP	All Internal	MEDIAtor	All High	Media range*
Application Sharing and File Transfer	TCP	MEDIAtor	All Internal	Media range*	All high
Application Sharing and File Transfer	TCP	All Internal	MEDIAtor	All High	Media range*

*) Media port range as configured on the MEDIAtor on the page SIP Service – Basic (default 58024-60999)

3 LCS Access Proxy configuration

For general information regarding how to set up an LCS see: "Live Communications Server 2005 Standard Edition Deployment Guide" that can be found at http://office.microsoft.com/en-us/FX011526591033.aspx

3.1 Access Proxy software installation

The software needed on the Access Proxy consists of a Windows Service that relays SIP-related information between the AP and firewall.

To install the service:

- Run the IgMediatorSetup.msi installation program.
- Click Next to close the welcome screen.
- Accept or change the installation folder. The default location is C:\Program Files\Ingate\IgMediator\ The option to install for "Everyone" or "Just me" is not significant. Leave the default.
  Click Next to continue.
- Confirm installation by clicking Next.
- Enter account information for the account that should be used to run the service, i.e. [DomainName]\Administrator
  IMPORTANT: The account must be a member of the "RTC Server Applications" group.
- Enter IP-address or host name and port of the firewall. Leave Detect NAT selected. A trace file for trace messages and a trace level between 0 and 4 can also be specified. See "Activation and configuration" for more information.
- Click Close to finish the installation.

At this point the software is installed but the service has not yet started.

3.2 Activation and configuration

The Ingate Mediator Service must be started manually the first time. It can then be set to be run automatically when the server boots. Note that the service depends on the Live Communication Server service. The Mediator service won't start unless the LCS service is running.

3.2.1 Starting the service

To start the Mediator service for the first time open the Computer Management console and open the Services node under Services and Applications. Select Ingate Mediator in the list of services and right-click to choose Properties from the menu. Here the service's settings can be revised and the service started.

When the service starts a single message is written to the Event Log. Other log messages are written to the trace file specified in the registry.

3.2.2 Changing settings

Settings for the Mediator service is in the Windows registry under the key HKEY_LOCAL_MACHINE\SOFTWARE\Ingate\Mediator. Changing the settings take effect only after restarting the service.

The address of the firewall is specified by entering either an ip-address or a hostname in MediatorAddess. The port is typically set to 5059.

To enable trace messages, set TraceLog to a filename and set TraceLevel to a value between 1 (errors only) and 4 (verbose). Set TraceLevel to 0 to turn tracing off.

4 Ingate configuration

The following settings should be made on the Ingate box.

4.1 General

Configure basic settings for management and networking including a default gateway.

4.2 LCS settings.

SIP SERVICES - BASIC

- ⇒ SIP module: On.
- ⇒ Open port 6891 for file transfer: On

SIP SERVICES – MEDIAtor

- ⇒ MEDIAtor: On.
- ⇒ IP address: Select the IP address and port used for communication with LCS Access Proxy. This should be the same IP address and port as selected in the LCS Access Proxy configuration.
- ⇒ Inside for media traversal: Select the internal interface
- ⇒ Outside for media traversal: Select the external interface

Done! Don't forget to apply the configuration.

5 Network Services and Architecture

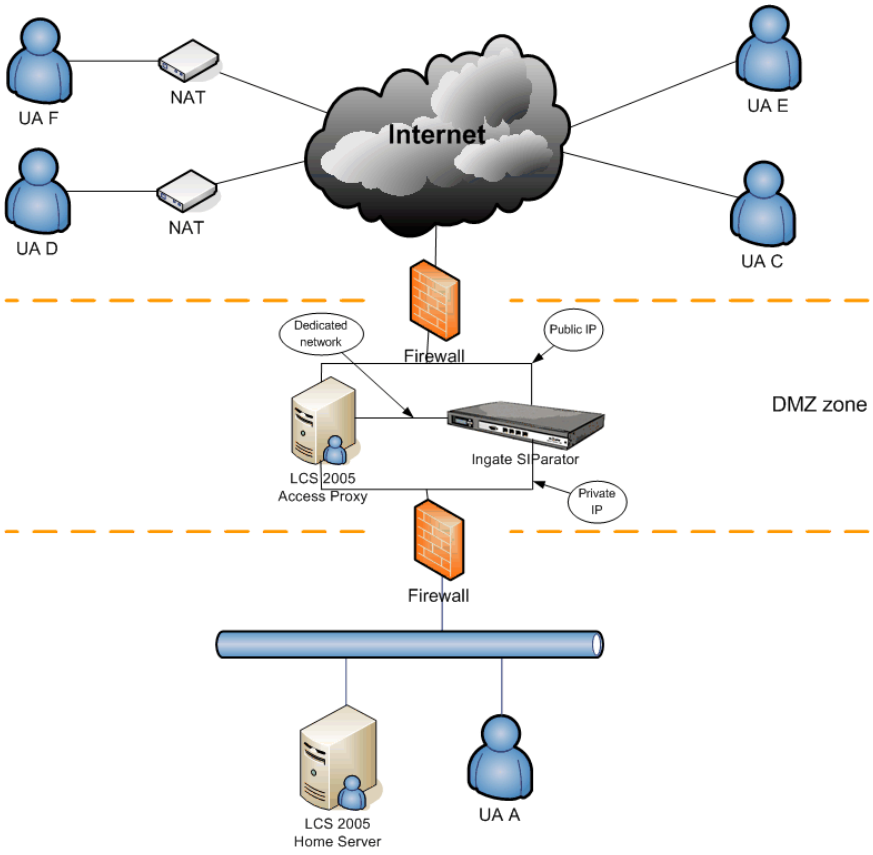
5.1 LCS

For LCS deployment see ”Live Communications Server 2005 Standard Edition Deployment Guide”, which can be found at http://office.microsoft.com/en-us/FX011526591033.aspx

5.2 Certificate Authority

For CA and certificate configuration in relation to LCS see ”Microsoft Office Live Communications Server 2005 Certificate Configuration”, which can be found at http://office.microsoft.com/en-us/FX011526591033.aspx

Appendix A. Functionality Matrix



Achieved functionality, transport = TLS

	A->C	A->D	C->A	C->D	C->E	D->A	D->C	D->F
Presence	OK	OK	OK	OK	OK	OK	OK	OK
IM	OK	OK	OK	OK	OK	OK	OK	OK
Multipart IM	OK	OK	OK	OK	OK	OK	OK	OK
Voice	OK	OK	OK	OK	OK	OK	OK	OK
Video	OK	OK	OK	OK	OK	OK	OK	OK
App. Sharing	OK	NOK	OK	NOK	OK	OK	NOK	NOK
Whiteboarding	OK	NOK	OK	NOK	OK	OK	NOK	NOK
File Transfer	NOK	NOK	NOK	NOK	OK	NOK	NOK	NOK

Comments to the functionality matrix:

1. Application Sharing and Whiteboarding uses a separate TCP session for data. The session is initiated by the calling party, and as it is not possible to initiate TCP sessions through a NAT device from the outside, these two applications will not work when the called party is located behind a non-SIP-aware NAT box.
2. File Transfer also uses TCP for data, but in this case the session is initiated by the called party. This means that it doesn't work when the calling party is located behind a non-SIP-aware NAT box.
3. File Transfer using TLS is currently not supported by Ingate. Some support is planned for the spring 2006.

The diagram below describes the call set-up for Application Sharing, Whiteboarding and File Transfer.