

# Microsoft® Lync<sup>™</sup>Server</mark>2010

# **Comunicaciones Unificadas**

Publicación EDGE Server con TMG 2010 Microsoft Most Valuable Professional



Compartiendo Experiencia Windows, Linux y mas...



# Comunicaciones Unificadas Virtualizadas

 En la siguiente presentación se realizara la publicación del rol EDGE Server en Lync Server 2010 con TMG 2010

Requisitos:

Lync Server 2010 Standard

- Lync 2010 FrontEnd (Instalado)
- Lync 2010 EDGE (Instalado) <u>http://bit.ly/LyncEDGE</u>
- TMG 2010
- DNS Publico
- Software Utilizado:
  - Windows 2008 R2 Datacenter / Enteprise (VMs)
  - Lync Server 2010





Nombre	Hardware Virtual	Redes	Roles			
DC01	512 MB RAM 2 vCPU 40 GB Disco	LAN: 192.168.50.1	Domain Controler RootCA / DNS			
LYFE01	2 GB RAM 2 vCPU 127 GB Disco	LAN: 192.168.50.5	Front End / Backend Mediation Server			
LYED01	2 GB RAM 2 vCPU 127 GB Disco	LAN: 192.168.50.15 DMZ: 10.1.0.2 DMZ: 10.1.0.3 DMZ: 10.1.0.4	Lync Standard EDGE			
EX01	2 GB RAM 2 vCPU 127 GB Disco	LAN: 192.168.50.20	Exchange 2010 SP2 HUB / CAS / MBX / UM			
Asterisk	2 GB RAM 2 vCPU 40 GB Disco	LAN: 192.168.50.220	Asterisk 1.8 PBX			
TMG01	2 GB RAM 2 vCPU 40 GB Disco	LAN: 192.168.50.100 DMZ: 10.1.0.1 WAN: 192.168.199.20/23	Firewall DNS Publico			
Win7	2 GB RAM 2 vCPU 127 GB Disco	LAN: 192.168.50.201	Cliente Lync en Dominio			
Win7ED	2 GB RAM 2 vCPU 127 Gb Disco	DMZ: 10.1.0.10	Cliente Lync en Workgroup			
Nota:	Nota: En el laboratorio todos los discos son de espacio dinámico (crece en funciona de la necesidad)					



# Esquema Funcional de la instalación







Agregamos los siguientes registros en nuestro DNS Publico IPs a EDGE Server edge.itsanchez.com.ar 192.168.199.20 webconf.itsanchez.com.ar 192.168.199.21 av.itsanchez.com.ar 192.168.199.22

## **IPs a Reverse Proxy**

sip.itsanchez.com.ar 192.168.199.23 dialin.itsanchez.com.ar 192.168.199.23 meet.itsanchez.com.ar 192.168.199.23

edge	Host (A)	192.168.199.20
webconf	Host (A)	192.168.199.21
av	Host (A)	192.168.199.22
i sip	Host (A)	192.168.199.23
meet	Host (A)	192.168.199.23
🗐 dialin	Host (A)	192.168.199.23

NOTA: las IPs publicas son privadas ya que se utiliza un laboratorio para validar funcionalidad en producción deben ser 4 IPs Publicas.



En nuestro dominio publico (itsanchez.com.ar), agregamos el registro SRV \_sipinternaltIs para en inicio automático

_sipinternaltls Prope	erties		<u>? ×</u>
Service Location (SRV	0		
Domain:	itsanchez.com.ar		
Service:	_sipinternaltls		<b>_</b>
Protocol:	_tcp		~
Priority:	0		
Weight:	0		
Port number:	443		
Host offering this se	rvice:		
edge.itsanchez.co	m.ar		
		1	
Ok	Cancel	Apply	Help



Las reglas que debemos agregar en nuestro firewall son las siguientes:

Compartiendo Experiencia Windows, Linux y mas...

1.com.37

Regla	IP Publica	IP Privada	Interface	Puertos y Protocolos
Acceso EDGE (Clientes)	192.168.199.20	10.1.0.2	DMZ	TCP – 443
Acceso EDGE (Federacion)	192.168.199.20	10.1.0.2	DMZ	TCP - 5061
Conferencias WEB EDGE	192.168.199.21	10.1.0.3	DMZ	TCP -443
A/V EDGE	192.168.199.22	10.1.0.4	DMZ	TCP – 443
A/V EDGE	192.168.199.22	10.1.0.4	DMZ	UDP - 3478
A/V EDGE	192.168.199.22	10.1.0.4	DMZ	TCP – 50.000 a 59.999
A/V EDGE	192.168.199.22	10.1.0.4	DMZ	UDP - 50.000 a 59.999
<b>Reverse Proxy</b>	192.168.199.23	192.168.50.5	LAN	TCP -443

NOTA: las IPs publicas son privadas ya que se utiliza un laboratorio para validar funcionalidad en producción deben ser 4 IPs Publicas.





Vamos a crear las reglas de publicación para Lync Server 2010 la primera que vamos a crear es reverse proxy, desde la consola de TMG



## Seleccionar -> Firewall Policy -> Publish Now-Web Server Protocols

🕮 Forefront TMG					
File Action View Help					
🗢 🧼 🖄 📷 🛛 🖬 🖄 🔿	📀 🍠 🔁 🍕	? 🚰 🎎 🍺			
Microsoft Forefront Threat Managemen     Forefront TMG (TMG01)     Dashboard     Monitoring	Foref Threat	<b>ront</b> Management G	ateway 2010		Enterprise
Firewall Policy	All Firewall P				Toolbox Tasks Help
E-Mail Policy	Search	۶	Examples		
Intrusion Prevention System Remote Access Policy (VPN)	Order 🔺	Name	Action	Protocols	Firewall Policy Tasks
- Networking	1	Ping - WAN	🕜 Allow	🖳 PING	Publish Exchange Web
System	[B] <b>2</b>	DNS Publico	Allow	🖳 DNS Ser	Client Access
🤪 Update Center	🖃 💽 3	DMZ a Internet	Allow	🛺 All Outb	🔚 Publish <b>Mail</b> Servers
Troubleshooting			-		E Publish SharePoint Sites
	🗆 Web Access	Policy Group		n	🐑 Publish <b>Web</b> Sites
	🧖 4	LocalHost	Allow	All Outb	Protocols



Seleccionamos el nombre de la regla -> Next

New Server Publishing Rule \	Wizard	×
	Welcome to the New Server Publishing Rule Wizard	
	This wizard helps you create a new server publishing rule. Server publishing rules map incoming client requests to the appropriate internal server.	
	Server publishing rule name: Lync - Reverse Proxy	
	To continue, click Next.	
	< Back Next > Cance	



Direccion IP Front End Lync Server -> Next

Ne	w Server Publishing Rule Wizard	×
	Select Server Specify the network IP address of the server you are publishing.	$\mathbb{H}$
	Server IP address:	
	192 . 168 . 50 . 5 Browse	
-	( Paulo Next > Co	
	< Back Next > Ca	



### Seleccionamos -> HTTPS Server -> Next

New Server Publishing Rule Wizard	×
Select Protocol Select the protocol used by the published server.	
Selected protocol:	
ITTPS Server	Properties
	Ports
	New
< Back Next	Cancel



X

### Seleccionamos -> External -> Address..

#### New Server Publishing Rule Wizard

#### Network Listener IP Addresses

Select the network IP addresses on the Forefront TMG that will listen for requests intended for the published server.

Listen for requests from these networks:

Name	Selected IPs	<b>▲</b>
🗹 🌑 External	<all addresses="" ip=""></all>	
🔲 🚽 Internal	<all addresses="" ip=""></all>	
🗖 🛶 Local Host	<all addresses="" ip=""></all>	
🗖 📥 Perimeter	<all addresses="" ip=""></all>	
Quarantined VPN Clients	<all addresses="" ip=""></all>	-
	AIL ID A AAAAAAA	
		Address
	< Back	Next > Cancel



## Seleccionamos la ip publica correspondiente al reverse proxy -> Add

#### External Network Listener IP Selection × Listen for requests on: C All IP addresses on the Forefront TMG computer that are in the selected network. C Default IP addresses for network adapters on this network. If Network Load Balancing is enabled for this network, the default virtual IP address will be used. Specified IP addresses on the Forefront TMG computer in the selected network. Available IP Addresses Selected IP Addresses IP Address IP Address Server Server 192, 168, 199, 20 TMG01 Add > 192, 168, 199, 21 TMG01 < Remove 192, 168, 199, 22 TMG01 192, 168, 199, 23 TMG01 Add IP.... Cancel OK



### Seleccionamos -> OK

#### External Network Listener IP Selection

Listen for requests on:

- C All IP addresses on the Forefront TMG computer that are in the selected network
- O Default IP addresses for network adapters on this network. If Network Load Balancing is enabled for this network, the default virtual IP address will be used.
- Specified IP addresses on the Forefront TMG computer in the selected network

#### Available IP Addresses

Selected IP Addresses

X





## Seleccionamos -> Next

#### New Server Publishing Rule Wizard

#### Network Listener IP Addresses

Select the network IP addresses on the Forefront TMG that will listen for requests intended for the published server. X

Listen for requests from these networks:

Name	Selected IPs
🗹 🎯 Extemal	192.168.199.23
🔜 🖦 Internal	<all addresses="" ip=""></all>
🗖 👍 Local Host	<all addresses="" ip=""></all>
Perimeter	<all addresses="" ip=""></all>
Quarantined VPN Clients	<all addresses="" ip=""></all>
	Address



#### Seleccionamos -> Finish

New Server Publishing Rule Wizard

#### Completing the New Server Publishing Rule Wizard

You have successfully completed the New Server Publishing Rule Wizard. The new Server Publishing Rule will have the following configuration: X

Name: Lync Rever Published Sen 192.168.50 Published Sen HTTPS Sen Listen on: External To close the w	se Proxy /er: 5 /ice: ver ver		×
	< Back	Finish	Cancel



Sobre la regla -> Botón Derecho -> Properties

1	Lync Reverse Proxy	🥝 Allow	🕅 нтте	
		<b></b>	Properties	
<u>, 7,</u> 2	Ping - WAN		Delete	
	DMC D. Lt.	🥟 all		
<u></u>	DINS PUDICO		Сору	
			1.4	

## En la solapa traffic -> Ports...

Allow network traffic using the following protocol:	
HTTPS Server	Properties
	Filtering
	Ports
	New



### Seleccionamos -> Published Server Ports -> 4443 -> OK

Ports	×
The port override options let you override the default ports used to a to the published server.	connect
Firewall Ports	
Publish using the default port defined in the protocol definition	
C Publish on this port instead of the default port:	Ě
Published Server Ports	
C Send requests to the default port on the published server	
• Send requests to this port on the published server:	÷
Source Ports	
<ul> <li>Allow traffic from any allowed source port</li> </ul>	
C Limit access to traffic from this range of source ports:	
From: To:	×
This range must belong to clients specified in the allowed traf sources for this rule.	fic
ОК	Cancel



En la solapa -> To -> Request appear to come from the Forefront TMG Computer -> OK

Lync Reverse Proxy Properties
General Action Traffic From To Networks Schedule
Specify the network address of the server to publish:
192 . 168 . 50 . 5 Browse
Requests for the published server Specify how Forefront TMG forwards requests to the published server:
<ul> <li>Requests appear to come from the Forefront TMG computer</li> <li>Requests appear to come from the original client</li> </ul>
OK Cancel Apply



## Confirmamos la regla con -> Apply

Forefront Threat Management Gateway 2010



Discard To save

To save changes and update the configuration, click Apply.

Describimos el cambio -> Apply -> Ok

Type a description for the applied changes. The	description is displayed in the change tracking en
Change description:	
Reverse Proxy - Lync	
Export You can click Export to back up	p the entire configuration
before applying the changes.	



Debemos generar tres (3) reglas adicionales vamos a repetir el mismo procedimiento modificando los puertos como se muestra en el detalle Regla Lync EDGE



Vemos las propiedades (Properties) en la solapa Traffic al crear la regla ponemos New y la configuramos igual que en la próxima pantalla

Lync - EDGE Properties	×
General Action Traffic From To Networks	Schedule
Allow network traffic using the following protocol:	
Lync - EDGE	Properties
	Filtering
	Ports
	New



# Seleccionamos la solapa -> Parameters

ync - EDGE Propei	rties
General Paramete	ers
-	
Name:	Lync - EDGE
Description	
(optional):	
	,
- Associated Stan	dard Protocol
C Associate th	is protocol definition with this standard protocol:
Troffic motor	ed to the protocol definition will be increated by
signatures co	prresponding to the associated standard protocol.
Garat	sinte a standard costs of with this costs of d.C. We
<ul> <li>Do not asso</li> </ul>	cate a standard protocol with this protocol definition
	OK Cancel Apply



## Deben estar los puertos 443 (TCP) y 5061 (TCP) -> OK

- EDGE Propert	ies			×
eral Parameter	s			
imary Connectio				
Timery connectio				
Port Range	Protocol Type	Direction	Add	
443 5051	TCP	Inbound	Edit,	
5061	TCP	Inbound		
			Remove	
econdary Conner	tions			
econdary connec	luons	1		
Port Range	Protocol Type	Direction	Add	
			Edit	
			Remove	
				·
pplication Filters				
DNS Filter				
FTP Access F	ilter			
H.323 Filter			<b>T</b>	
	ected application (	filters		
i show only se		niter s		
		OK 1	Concel Conclu	



Validamos en la solapa Networks la IP Publica Correspondiente 192.168.199.20 EDGE

Lync - EDGE Properties	×
General Action Traffic From To	Networks Schedule
Selected networks for this listener:	
Name	Selected IPs
🗹 🌑 External	192.168.199.20
🔲 📥 Internal	<all addresses="" ip=""></all>
Local Host	<all addresses="" ip=""></all>
Penmeter     Puscentined VPN Cliente	<all addresses="" ip=""></all>
VPN Clients	<all addresses="" ip=""></all>
All Networks (and Local	<all addresses="" ip=""></all>
All Protected Networks	<all addresses="" ip=""></all>
🗖 🍰 Forefront Protection Man	<all addresses="" ip=""></all>
	Address
	Cancel Apply
	Cancer Apply



# Validamos en la solapa **TO** que el trafico se envie al la IP DMZ Correspondiente **10.1.0.2 EDGE -> OK**

y	ync - EDGE Properties
	General Action Traffic From To Networks Schedule
	Specify the network address of the server to publish:
	10.1.0.2 Browse
	Requests for the published server
	Specify how Forefront TMG forwards requests to the published server:
	C Requests appear to come from the Forefront TMG computer
	Requests appear to come from the original client
	OK Canad L Apply
	Cancel Apply



Regla Lync WEBCONF, es igual a la de reverse proxy con otra IP Publica

3 1	Lync - WEBCONF	🧭 Allow	🛄 нтте
	Luna EDCE	Properties	
	2 Lync - EDGE	Delete	ync
[8] 3	Exchange - OWA		TTF

Vemos las propiedades (**Properties**) en la solapa **Traffic** al crear la regla ponemos New y la configuramos igual que en la próxima pantalla

Constitutes Toffic Law IT. INcontain Constant				
General Action Hallic From To Networks Schedule				
Allow network traffic using the following protocol:				
HTTPS Server   Properties				
Filtering				
Ports				
New				
New				



# Validamos en la solapa **TO** que el trafico se envie al la IP DMZ Correspondiente **10.1.0.3 WEBCONF**

Lync - WEBCONF Properties	×
General Action Traffic From To Networks Schedule	
Specify the network address of the server to publish:	
10 . 1 . 0 . 3 Browse	
Requests for the published server	
Specify how Forefront TMG forwards requests to the published server:	
C Requests appear to come from the Forefront TMG computer	
Requests appear to come from the original client	
OK Cancel Apply	



# Validamos en la solapa **TO** que el trafico se envie al la IP DMZ Correspondiente **10.1.0.3 WEBCONF**

Lync - WEBCONF Properties	×		
General Action Traffic From To Networks Schedule			
Specify the network address of the server to publish:			
10 . 1 . 0 . 3 Browse			
Requests for the published server			
Specify how Forefront TMG forwards requests to the published server:			
C Requests appear to come from the Forefront TMG computer			
Requests appear to come from the original client			
OK Cancel Apply			



Validamos en la solapa Networks la IP Publica Correspondiente 192.168.199.21 WEBCONF

Lync - WEBCONF Properties	×		
General Action Traffic From To	Networks Schedule		
Selected networks for this listener:			
Name	Felected IPs		
🗹 🌑 External	192.168.199.21		
🗖 📥 Internal	<all addresses="" ip=""></all>		
	<all addresses="" ip=""></all>		
Perimeter	<all addresses="" ip=""></all>		
	<all addresses="" ip=""></all>		
All Networks (and Local	<all addresses="" ip=""></all>		
All Protected Networks	<all addresses="" ip=""></all>		
🗖 🄹 Forefront Protection Man	<all addresses="" ip=""></all>		
	Address		
	Address		
ОК	Cancel Apply		



Regla Lync AV, es la que requiere mas puertos y veremos su configuración en detalle



Vemos las propiedades (Properties) en la solapa Traffic al crear la regla ponemos New y la configuramos igual que en la próxima pantalla

General Action Traffic From To Networks Schedule	
Allow network traffic using the following protocol:	
Lync AV   Properties	
Filtering	
Ports	
New	



# Validamos los puertos utilizados por Lync

Lync AV Properti	ies		×	
General Param	eters			
			[	
Primary Conne	ctions			
Port Range	Protocol Type	Direction	Add	
443	TCP	Inbound	Edit	
50000-59999		Indound		
30000-3333		Receive	Remove	
Secondary Cor	prections			
Secondary Cor	inections		(	
Port Range	Protocol Type	Direction	Add	
			Edit	
			Remove	
			- INDINGYO	
- Application Filt				
Application Flit	ers		-	
DNS Filter	DNS Filter			
FTP Access Filter				
Show only selected application filters				
	Г	OK Cano	el Apply	
	_			



En la solapa **To** configuramos la IP DMZ correspondiente a **Lync AV 10.1.0.4** 





En la solapa Networks configuramos la IP Publica correspondiente a Lync AV 192.168.199.22

Lync AV Properties	×			
General Action Traffic From To Networks Schedule Selected networks for this listener:				
Name	Selected IPs 192.168.199.22 <all addresses="" ip=""> <all addresses="" ip=""></all></all></all></all></all></all></all></all></all></all>			
	Address			



Con esta configuración los clientes de Lync, pueden conectarse si se importa el certificado de la RootCA Privada utilizada en la configuración para terminar con todas las funcionalidades y permitir federar con mensajería publica se deben comprar 2 certificados SAN Públicos (EDGE, Reverse Proxy)

0 📑 🤊 🖃	Bandeja de entrada - gsanchez@itsan	📕 Microsoft Lync	
File Home Send / R	eceive Folder View	What's happening today?	
<ul> <li>✓ Favorites</li> <li>✓ Bandeja de entrada</li> <li>✓ Correo sin leer</li> <li>✓ Elementos enviados</li> <li>✓ Elementos eliminados</li> </ul>	Search Bandeja de entrada (Ctrl+E) Arrange By: Date Today	Guillermo Sanchez Available * Set Your Location *	
<ul> <li>✓ gsanchez@itsanchez.com.ai</li> <li>☑ Bandeja de entrada</li> <li>☑ Borradores</li> </ul>	Guillermo Sanchez Prueba Nuevo Grupo Todos	Find a contact or dial a number     Image: Contact or dial a number       Groups     Status     Relationship	
<ul> <li>Elementos enviados</li> <li>Elementos eliminados</li> <li>Bandeja de salida</li> </ul>		<ul> <li>Frequent Contacts</li> <li>Frequent contacts are automatically added to this</li> <li>All Contacts (0/2)</li> <li>Call</li> </ul>	
Conversation History  Correo no deseado  RSS Feeds	Prueba Nuevo Grupo Todos Guillermo Sanchez	LyncUser01 - Offline	
Espero les sea de utilidad!!			

Saludos

Guillermo Sanchez

gsanchez@itsanchez.com.ar