



Microsoft®
Lync™ Server 2010

Comunicaciones Unificadas

Publicación EDGE Server
con TMG 2010



ITSanchez.com.ar
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) <http://bit.ly/LyncEDGE>
 - TMG 2010
 - DNS Publico
- **Software Utilizado:**
 - Windows 2008 R2 Datacenter / Enterprise (VMs)
 - Lync Server 2010



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Nombre	Hardware Virtual	Redes	Roles
DC01	512 MB RAM 2 vCPU 40 GB Disco	LAN: 192.168.50.1	Domain Controller 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

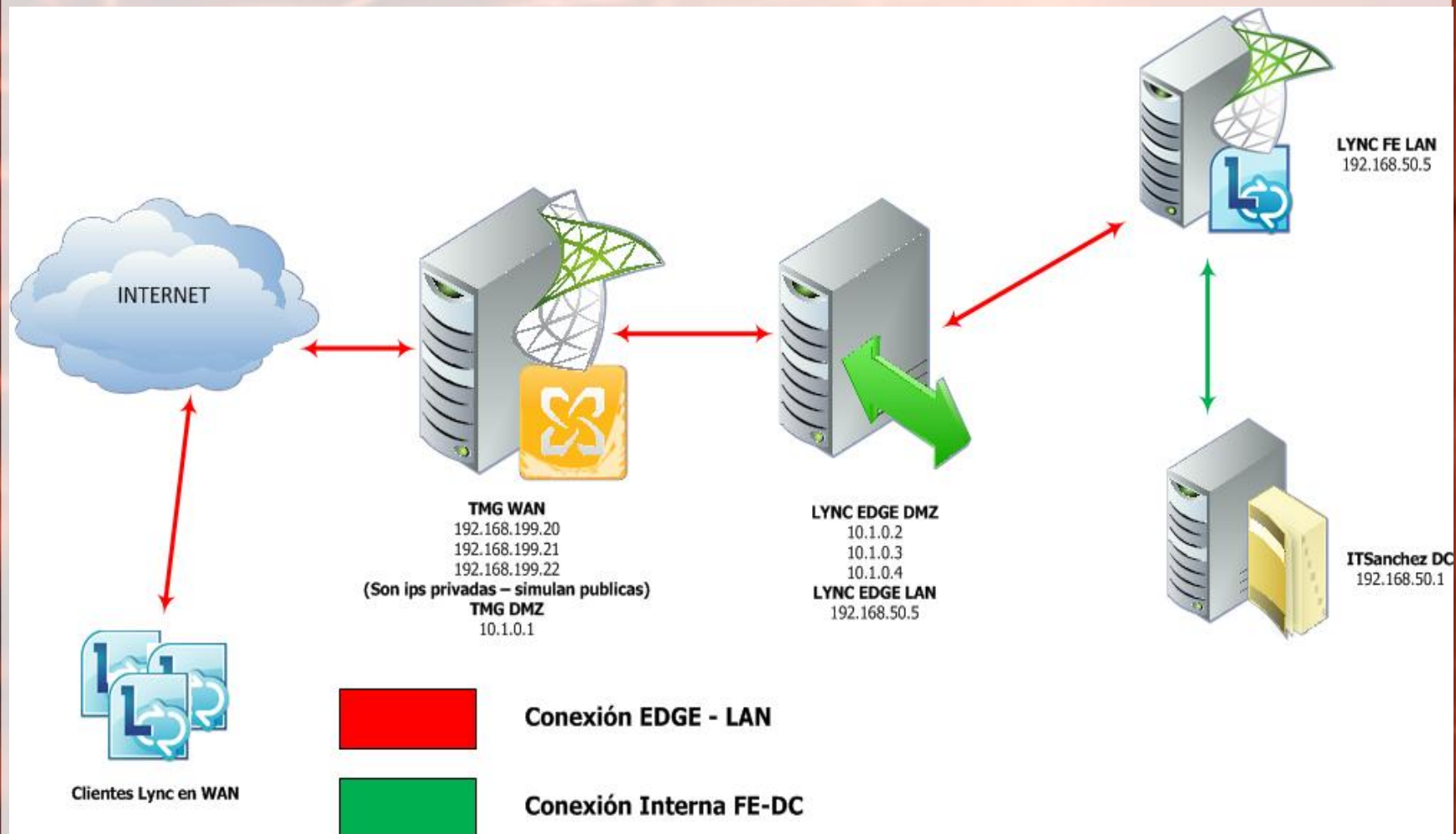
Nota: En el laboratorio todos los discos son de espacio dinámico (crece en funcion de la necesidad)



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Esquema Funcional de la instalación





ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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
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.



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

_sipinternaltls Properties [?] [X]

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

OK Cancel Apply Help



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

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
Reverse Proxy	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.



ITSanchez.com.ar

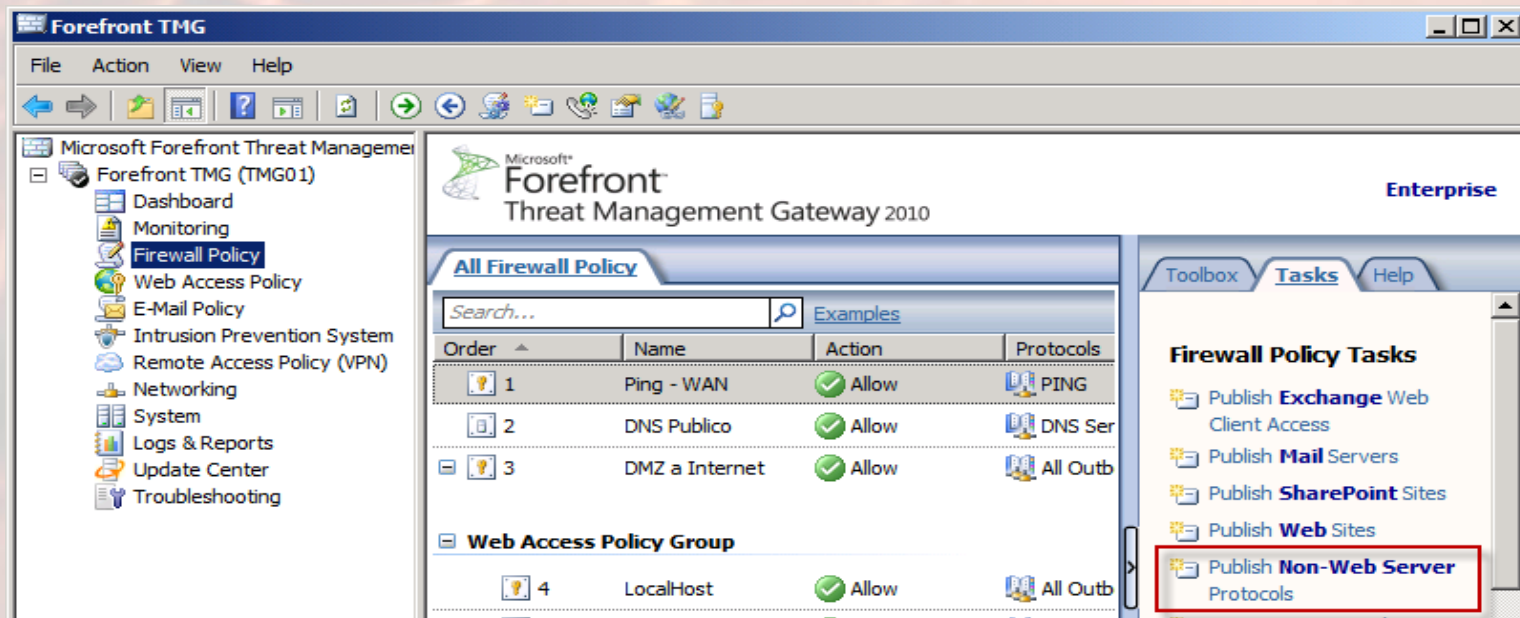
Compartiendo Experiencia
Windows, Linux y mas...

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



Forefront TMG Management

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





ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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 >** Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Direccion IP Front End Lync Server → **Next**

New Server Publishing Rule Wizard [X]

Select Server
Specify the network IP address of the server you are publishing.

Server IP address:



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Seleccionamos -> HTTPS Server -> Next

New Server Publishing Rule Wizard [X]

Select Protocol
Select the protocol used by the published server.

Selected protocol:

HTTPS Server [v]

Properties...
Ports...
New...

< Back **Next >** Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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
<input checked="" type="checkbox"/> External	<All IP addresses>
<input type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	<All IP addresses>
<input type="checkbox"/> Perimeter	<All IP addresses>
<input type="checkbox"/> Quarantined VPN Clients	<All IP addresses>
<input type="checkbox"/> VPN Clients	<All IP addresses>

Address...

< Back Next > Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

External Network Listener IP Selection

Listen for requests on:

- ☐ All IP addresses on the Forefront TMG computer that are in the selected network
- ☐ 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

IP Address	Server
192.168.199.20	TMG01
192.168.199.21	TMG01
192.168.199.22	TMG01
192.168.199.23	TMG01

Selected IP Addresses

IP Address	Server
------------	--------

Add >

< Remove

Add IP...

OK Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Seleccionamos → OK

External Network Listener IP Selection [X]

Listen for requests on:

- ☐ All IP addresses on the Forefront TMG computer that are in the selected network
- ☐ 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

IP Address	Server
192.168.199.20	TMG01
192.168.199.21	TMG01
192.168.199.22	TMG01

Selected IP Addresses

IP Address	Server
192.168.199.23	TMG01

Buttons: Add > < Remove Add IP... OK Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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.

Listen for requests from these networks:

Name	Selected IPs
<input checked="" type="checkbox"/> External	192.168.199.23
<input type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	<All IP addresses>
<input type="checkbox"/> Perimeter	<All IP addresses>
<input type="checkbox"/> Quarantined VPN Clients	<All IP addresses>
<input type="checkbox"/> VPN Clients	<All IP addresses>

Address...

< Back **Next >** Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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:

Name:
Lync Reverse Proxy

Published Server:
192.168.50.5

Published Service:
HTTPS Server

Listen on:
External

To close the wizard, click Finish.

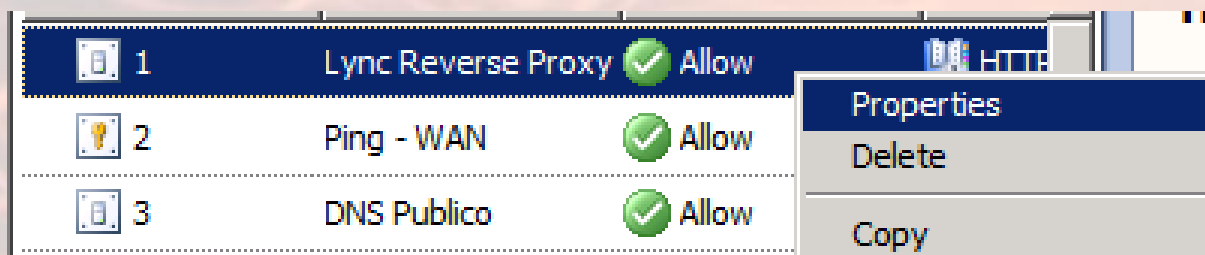
< Back **Finish** Cancel



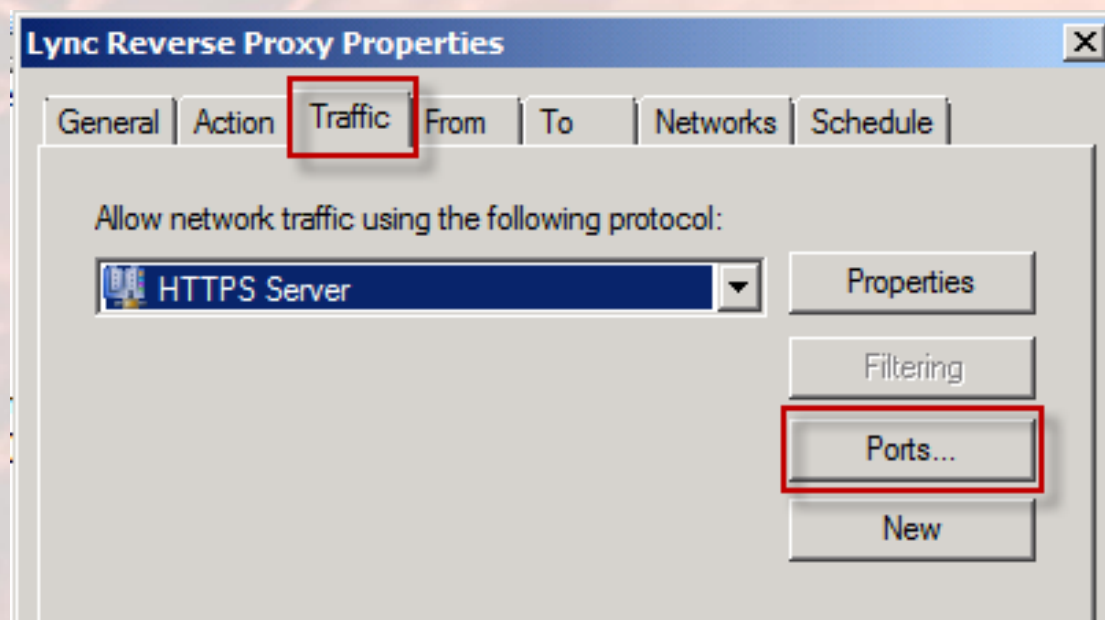
ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Sobre la regla -> Botón Derecho -> Properties



En la solapa traffic -> Ports...





ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

Ports [X]

The port override options let you override the default ports used to connect to the published server.

Firewall Ports

☒ Publish using the default port defined in the protocol definition

☐ Publish on this port instead of the default port: []

Published Server Ports

☐ Send requests to the default port on the published server

☒ Send requests to this port on the published server: **4443**

Source Ports

☒ Allow traffic from any allowed source port

☐ Limit access to traffic from this range of source ports:

From: [] To: []

This range must belong to clients specified in the allowed traffic sources for this rule.

OK Cancel



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

Lync Reverse Proxy Properties [X]

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:

☒ Requests appear to come from the Forefront TMG computer

☐ Requests appear to come from the original client

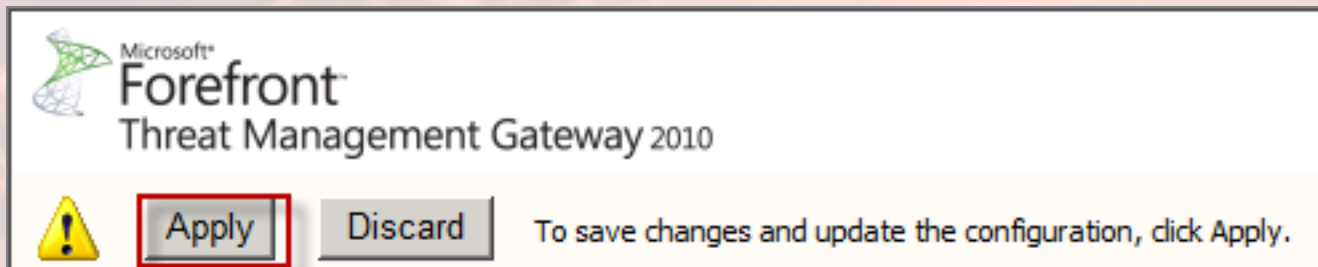
[OK] [Cancel] [Apply]



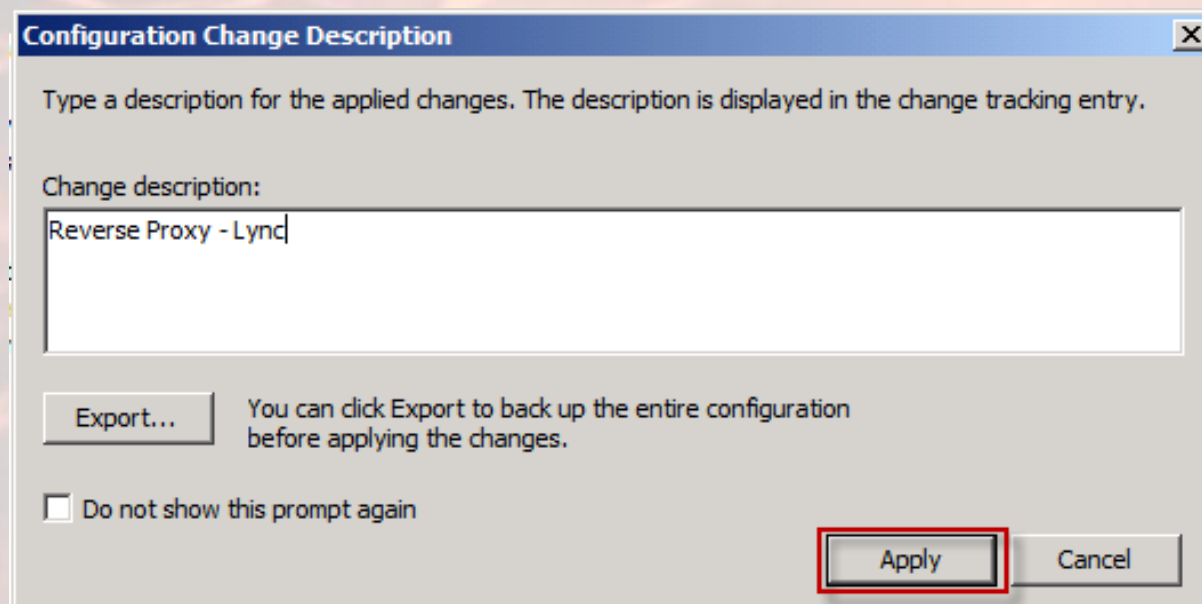
ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Confirmamos la regla con -> **Apply**



Describimos el cambio -> **Apply -> Ok**



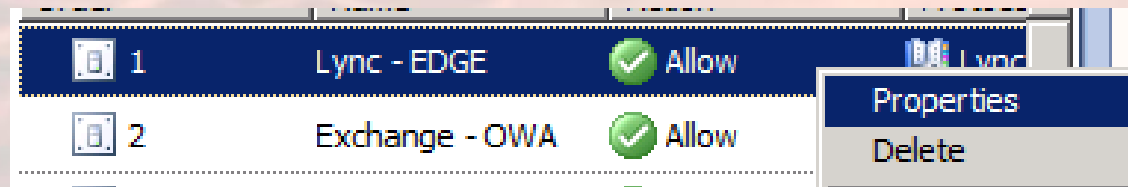


ITSanchez.com.ar

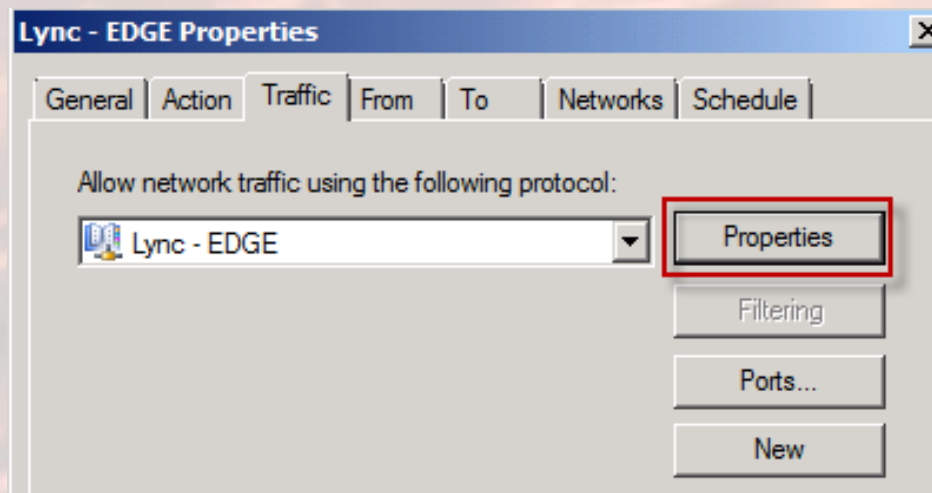
Compartiendo Experiencia
Windows, Linux y mas...

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






ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Seleccionamos la solapa -> **Parameters**

Lync - EDGE Properties [X]

General **Parameters**

 Name:

Description (optional):

Associated Standard Protocol

☐ Associate this protocol definition with this standard protocol:

Traffic matched to the protocol definition will be inspected by signatures corresponding to the associated standard protocol.

☒ Do not associate a standard protocol with this protocol definition

OK Cancel Apply



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

Lync - EDGE Properties

General Parameters

Primary Connections

Port Range	Protocol Type	Direction
443	TCP	Inbound
5061	TCP	Inbound

Add... Edit... Remove

Secondary Connections

Port Range	Protocol Type	Direction
------------	---------------	-----------

Add... Edit... Remove

Application Filters

- ☐ DNS Filter
- ☐ FTP Access Filter
- ☐ H.323 Filter
- ☐ MMC Filter

☐ Show only selected application filters

OK Cancel Apply



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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
<input checked="" type="checkbox"/> External	192.168.199.20
<input type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	<All IP addresses>
<input type="checkbox"/> Perimeter	<All IP addresses>
<input type="checkbox"/> Quarantined VPN Clients	<All IP addresses>
<input type="checkbox"/> VPN Clients	<All IP addresses>
<input type="checkbox"/> All Networks (and Local ...	<All IP addresses>
<input type="checkbox"/> All Protected Networks	<All IP addresses>
<input type="checkbox"/> Forefront Protection Man...	<All IP addresses>

Address...

OK Cancel Apply



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Validamos en la solapa **TO** que el trafico se envíe a la IP DMZ
Correspondiente **10.1.0.2 EDGE -> OK**

Lync - EDGE Properties [X]

General | Action | Traffic | From | **To** | Networks | Schedule

Specify the network address of the server to publish:

. . .

Requests for the published server

Specify how Forefront TMG forwards requests to the published server:

☐ Requests appear to come from the Forefront TMG computer

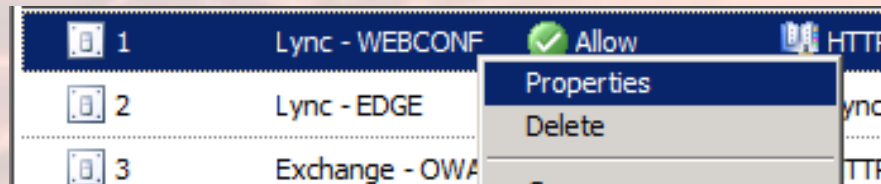
☒ Requests appear to come from the original client



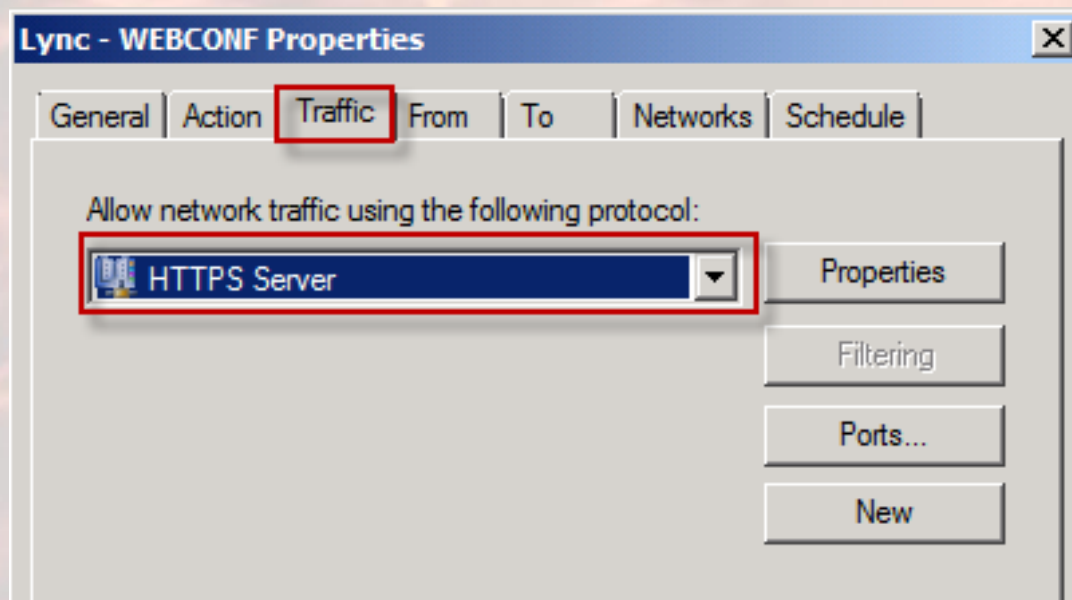
ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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



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





ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Validamos en la solapa **TO** que el trafico se envíe a 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:

Requests for the published server

Specify how Forefront TMG forwards requests to the published server:

☐ Requests appear to come from the Forefront TMG computer

☒ Requests appear to come from the original client



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Validamos en la solapa **TO** que el trafico se envíe a 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:

Requests for the published server

Specify how Forefront TMG forwards requests to the published server:

☐ Requests appear to come from the Forefront TMG computer

☒ Requests appear to come from the original client



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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	Selected IPs
<input checked="" type="checkbox"/> External	192.168.199.21
<input type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	<All IP addresses>
<input type="checkbox"/> Perimeter	<All IP addresses>
<input type="checkbox"/> Quarantined VPN Clients	<All IP addresses>
<input type="checkbox"/> VPN Clients	<All IP addresses>
<input type="checkbox"/> All Networks (and Local ...	<All IP addresses>
<input type="checkbox"/> All Protected Networks	<All IP addresses>
<input type="checkbox"/> Forefront Protection Man...	<All IP addresses>

Address...

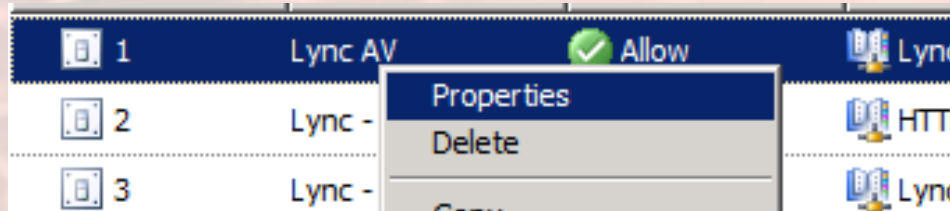
OK Cancel Apply



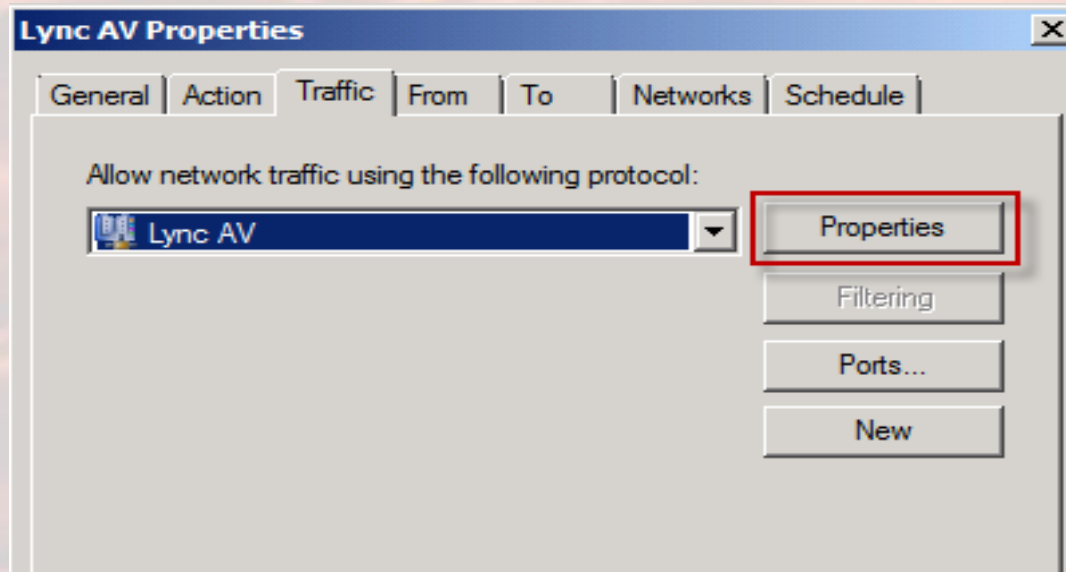
ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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





ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

Validamos los puertos utilizados por Lync

Lync AV Properties

General Parameters

Primary Connections

Port Range	Protocol Type	Direction
443	TCP	Inbound
50000-59999	TCP	Inbound
50000-59999	UDP	Receive

Add... Edit... Remove

Secondary Connections

Port Range	Protocol Type	Direction
------------	---------------	-----------

Add... Edit... Remove

Application Filters

- ☐ DNS Filter
- ☐ FTP Access Filter
- ☐ H.323 Filter
- ☐ MMS Filter

☐ Show only selected application filters

OK Cancel Apply



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

The screenshot shows the 'Lync AV Properties' dialog box with the 'To' tab selected. The 'To' tab is highlighted with a red box. Below the tab, the text 'Specify the network address of the server to publish:' is followed by an IP address field containing '10 . 1 . 0 . 4', which is also highlighted with a red box. To the right of the IP field is a 'Browse' button. Below this, there is a section titled 'Requests for the published server' with the instruction 'Specify how Forefront TMG forwards requests to the published server:'. There are two radio button options: 'Requests appear to come from the Forefront TMG computer' (unselected) and 'Requests appear to come from the original client' (selected). At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Lync AV Properties

General Action Traffic From **To** Networks Schedule

Specify the network address of the server to publish:

10 . 1 . 0 . 4 Browse

Requests for the published server

Specify how Forefront TMG forwards requests to the published server:

☐ Requests appear to come from the Forefront TMG computer

☒ Requests appear to come from the original client

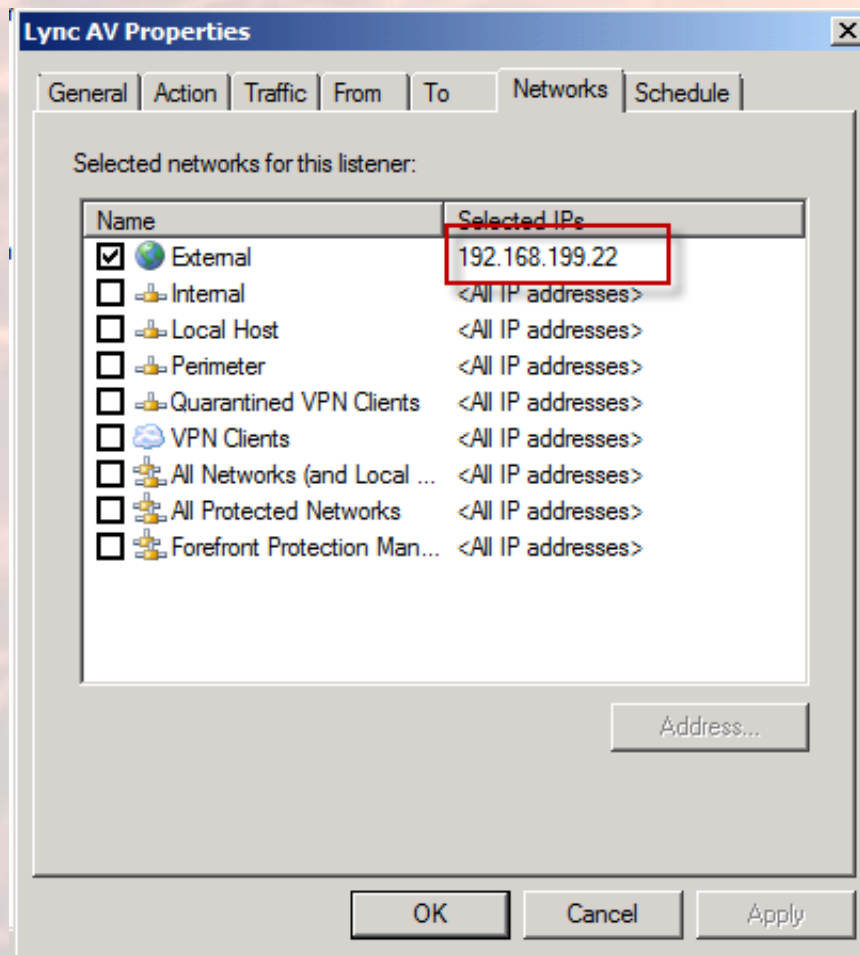
OK Cancel Apply



ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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

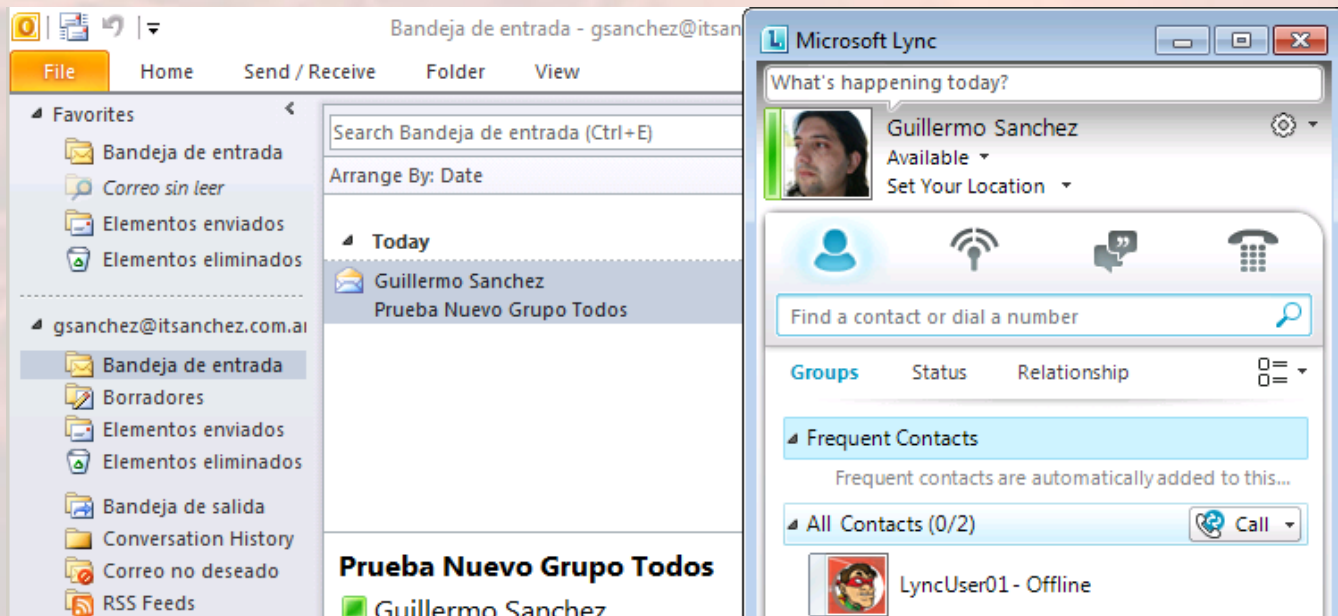




ITSanchez.com.ar

Compartiendo Experiencia
Windows, Linux y mas...

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)



Espero les sea de utilidad!!

Saludos

Guillermo Sanchez

gsanchez@itsanchez.com.ar