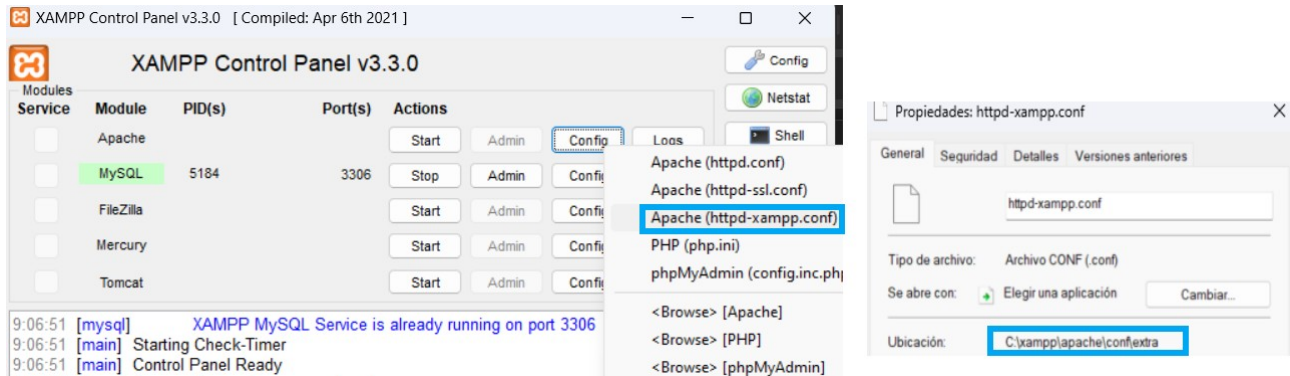


XAMPP PARA ACCESO REMOTO



Para permitir el acceso remoto al resto de equipos de nuestra red local, (con Apache apagado) debemos modificar nuestro archivo de configuración httpd-xampp.conf que se encuentra en xampp/Apache/conf/extra aunque es más rápido acceder desde el panel de control.



Dentro de este archivo, podemos modificar o añadir unas directivas personalizadas.

```
#
# New XAMPP security concept
#

# Proteger configuraciones y herramientas administrativas
<LocationMatch "^/(?:xampp|phpmyadmin|licenses|webalizer|server-status|server-
info|security)">
    Require ip 127.0.0.1
</LocationMatch>

# Proteger archivos sensibles en cualquier ubicación
<FilesMatch "^(?:\.htaccess|httpd\.conf|php\.ini|\.env|config\.php|\.bak|\.sql)$">
    Require ip 127.0.0.1
</FilesMatch>

# Exponer solo los sitios web
# Asegurarse de que el DocumentRoot de tus sitios (por ejemplo, /htdocs) esté accesible
<Directory "C:\xampp\htdocs">
    Require all granted
</Directory>
```

Con estos cambios de configuración protegemos algunos archivos de configuración o más críticos del acceso externo, però a su vez permitimos que se acceda al directorio htdocs que es el que usa el interprete de PHP en sus archivos internos.

Aitor Pascual Jiménez
Despliegue de Aplicaciones Web
2º DAW

En este momento ya podríamos levantar Apache.

Module	PID(s)	Port(s)	Actions
Apache	8708 532	80, 443	Stop

Si probamos a lanzar un curl desde otro equipo (en este caso el de mi compañera Marta).

```
C:\Users\AlumnoMañana.2DAW07>curl http://172.16.3.224/modulosPHP/POO/ClaseCalc.php
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
[+] La suma de numero1 -> 5 numero2 -> 6<br>[+] Es de -> 11</body>
</html>
C:\Users\AlumnoMañana.2DAW07> |
```

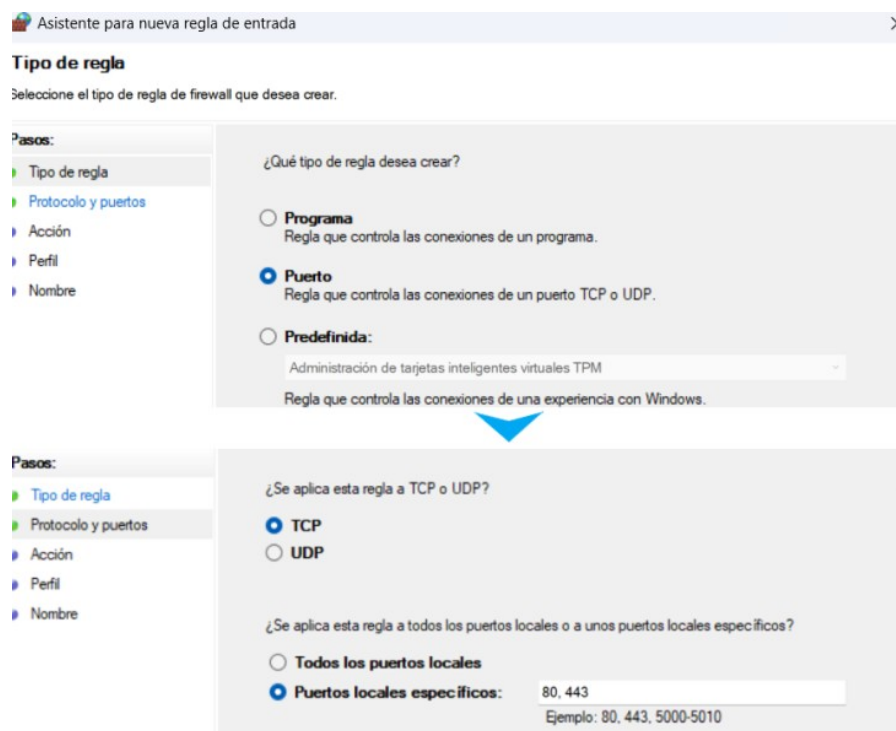
Podemos comprobar que este resuelve e interpreta correctamente.

A la hora de exponer nuestro Apache a internet, deberíamos abrir un puerto en nuestro router y aplicar unas directivas de seguridad en nuestro sistema, en mi caso no tengo acceso a la configuración del router de clase entonces he probado con un servicio externo, desgraciadamente ni siquiera haciendo uso de este servicio he conseguido tunelizar.

Las directivas de seguridad las aplicaremos desde el firewall.

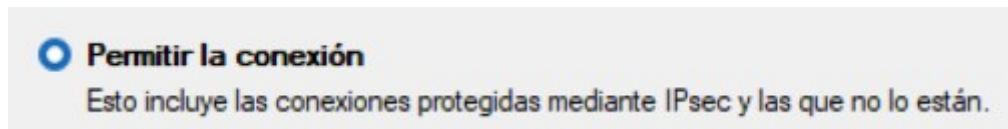


Tanto para entrada como para salida deberemos permitir acceso a los puertos 80 y 443 en caso de usar http y https en los puertos predeterminados (cosa recomendable en la gran mayoría de los casos).

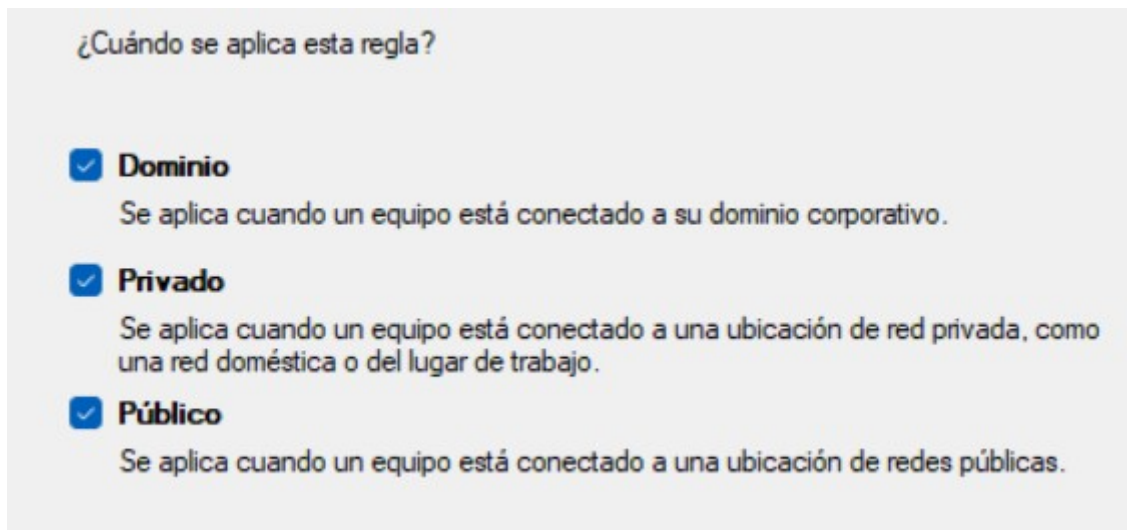


Aitor Pascual Jiménez
Despliegue de Aplicaciones Web
2º DAW

Permitimos la conexión.



En cualquier caso.



Usando de un servicio externo como <https://whatismyipaddress.com> podemos obtener nuestra ip pública.



Aitor Pascual Jiménez
Despliegue de Aplicaciones Web
2º DAW

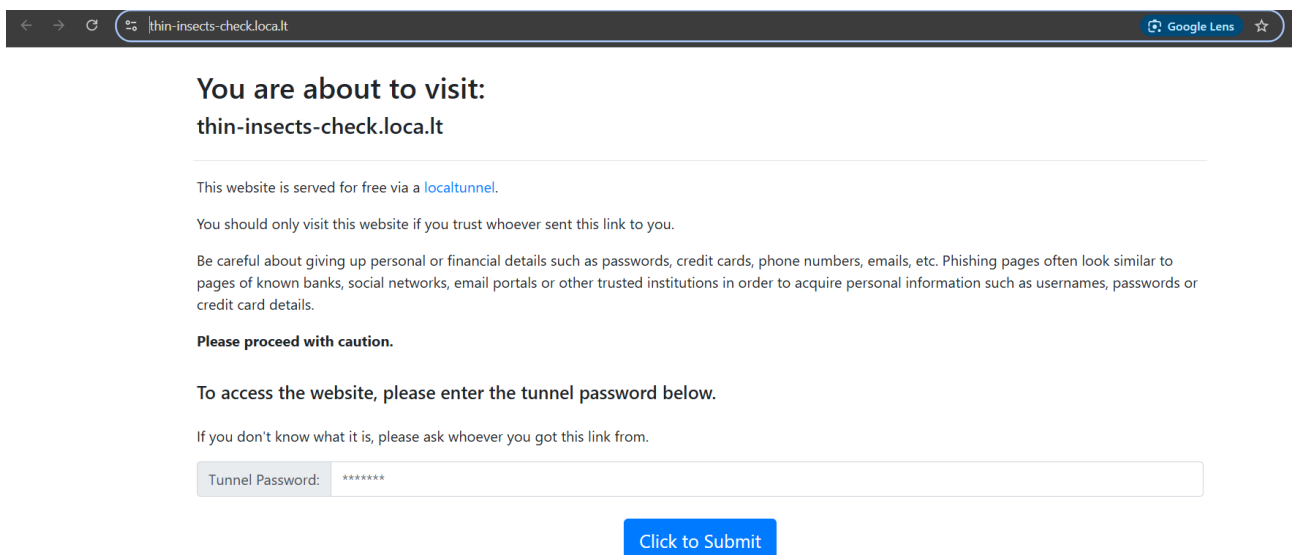
En mi caso en vez de hacer uso de Ngrok he probado la segunda alternativa más popular, que es localtunnel, he instalado esta dependencia de node de manera global.

```
D:\node>npm install -g localtunnel  
  
added 22 packages in 2s
```

Esta dependencia te permite externalizar el servicio que corre en un puerto.

```
C:\Users\aaaito\Documents\jakartaServer>lt -p 80  
your url is: https://thin-insects-check.loca.lt
```

En la página proporcionada debes introducir tu ip pública.



The screenshot shows a web browser window with the address bar displaying "thin-insects-check.loca.lt". The page content includes a warning message: "You are about to visit: thin-insects-check.loca.lt". Below this, it states: "This website is served for free via a localtunnel." and "You should only visit this website if you trust whoever sent this link to you." A cautionary note follows: "Be careful about giving up personal or financial details such as passwords, credit cards, phone numbers, emails, etc. Phishing pages often look similar to pages of known banks, social networks, email portals or other trusted institutions in order to acquire personal information such as usernames, passwords or credit card details." A bold instruction reads: "Please proceed with caution." Below this, it says: "To access the website, please enter the tunnel password below." and "If you don't know what it is, please ask whoever you got this link from." At the bottom, there is a text input field labeled "Tunnel Password:" with a masked password "*****" and a blue button labeled "Click to Submit".

Aitor Pascual Jiménez
Despliegue de Aplicaciones Web
2º DAW

El problema sucede al entrar ya que algún cortafuegos de alguno de los routers no nos permite comunicarnos correctamente y obtenemos un http 502.



502 Bad Gateway

nginx/1.17.9

502 Bad Gateway



502
Bad Gateway

Description

The HTTP **502 Bad Gateway** server error response code indicates that the server, while acting as a gateway or proxy, received an invalid response from the upstream server.