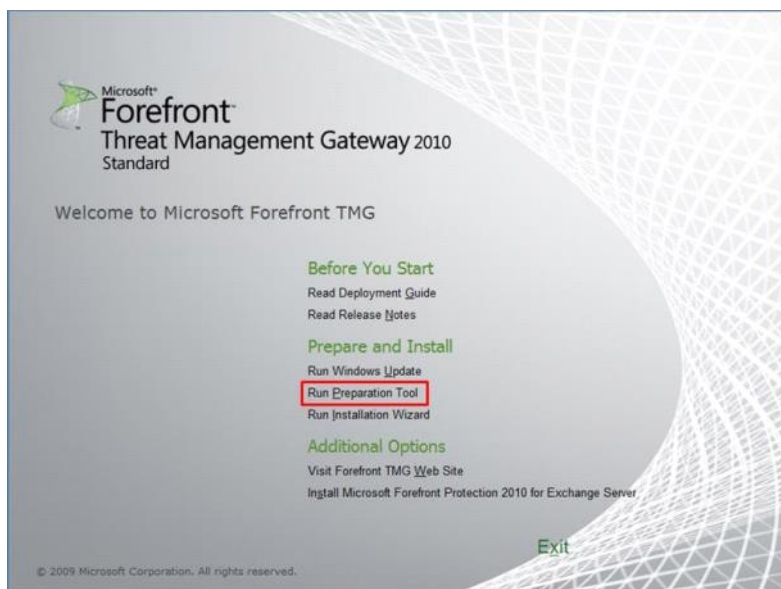
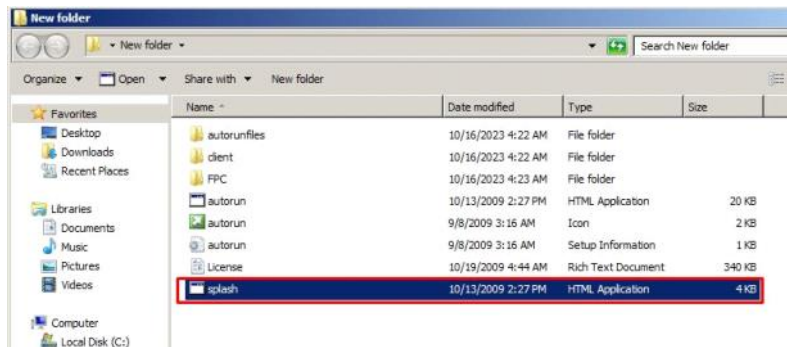


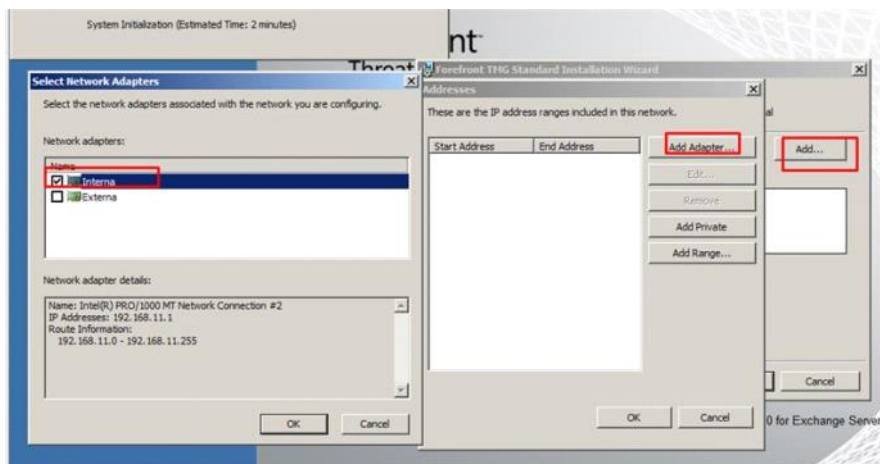
Forefront (firewall)

martes, 17 de octubre de 2023 9:04

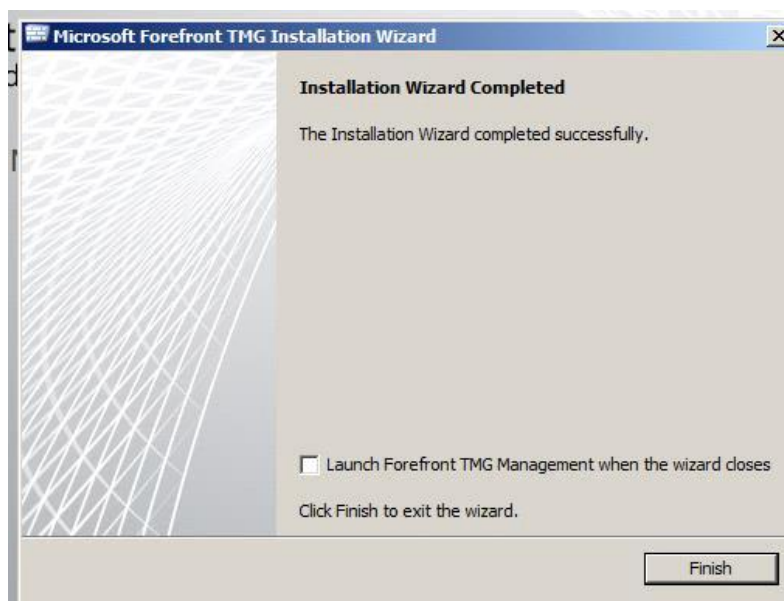
Ejecutamos la aplicación:



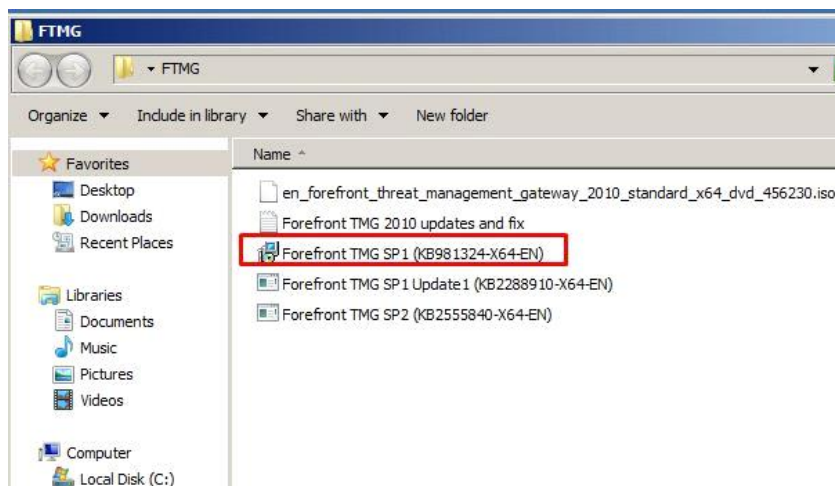
Aquí tenemos que meter el adaptador de la red interna



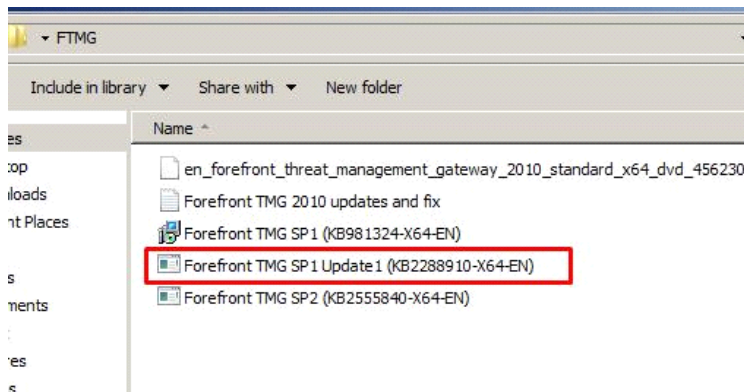
No marcar este cuadrado



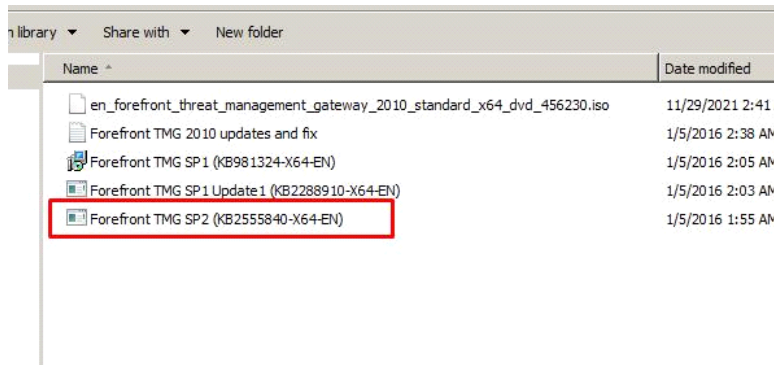
Después de la instalación ejecutar este programa y todo para adelante



Después instalamos el update 1

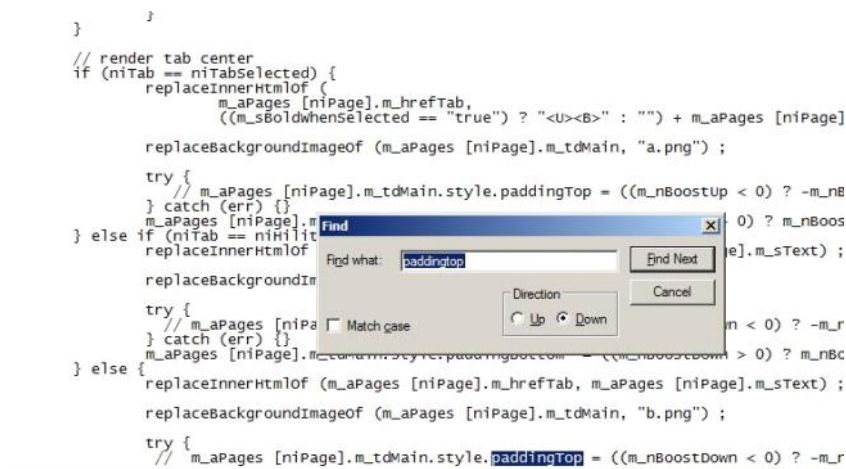


Y por último el 2



Entramos en tabsHandler

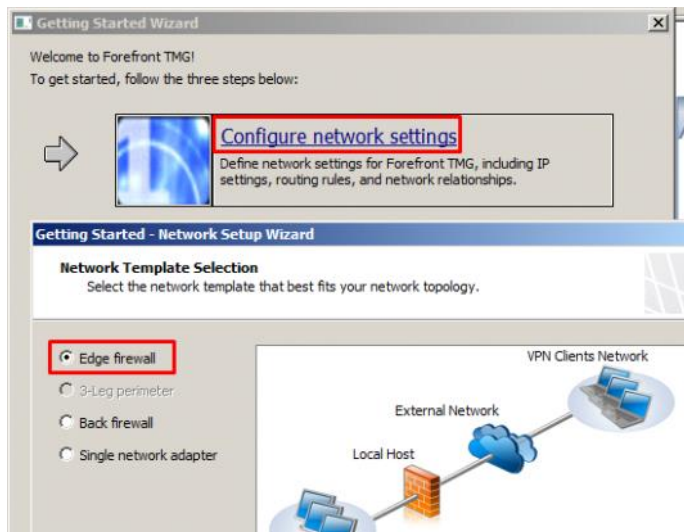
Buscar paddintop y comertalos con // (son 3 padding top) y guardamos el archivo:



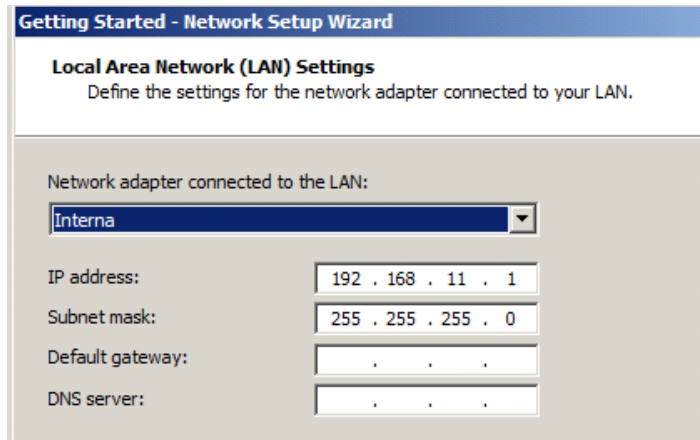
Anclamos al inicio el programa forefront y borramos las carpetas

-Configurar forefront:

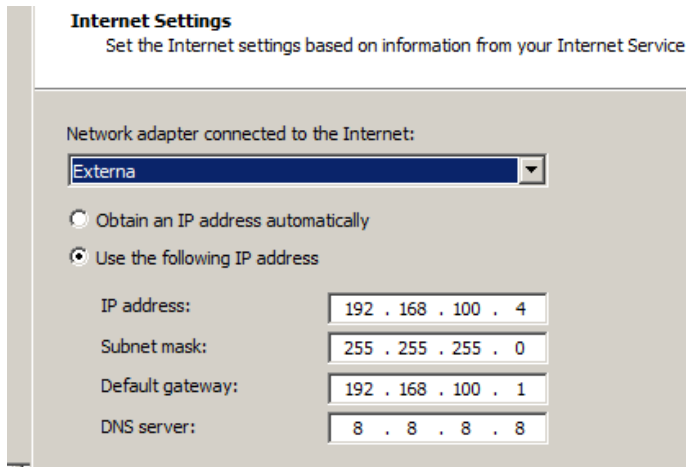
Paso 1:



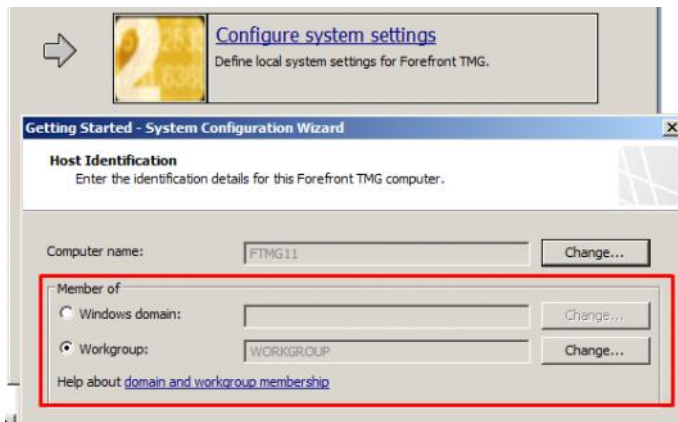
-Red interna:



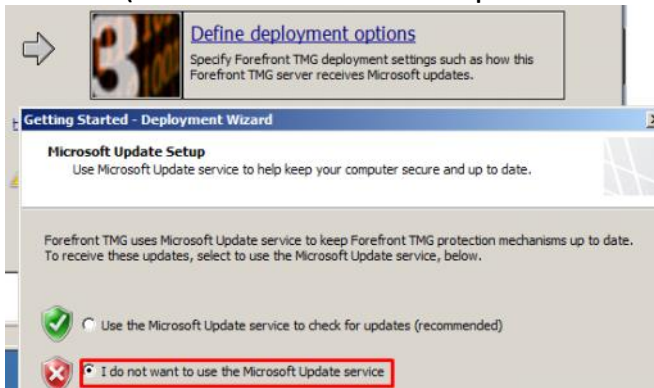
-Red externa:



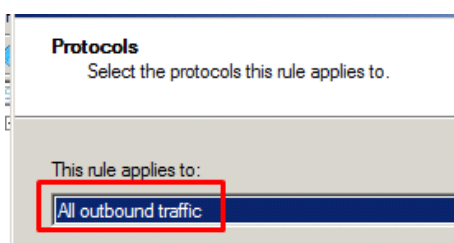
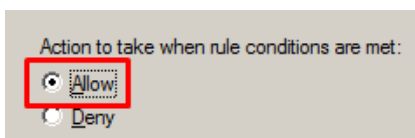
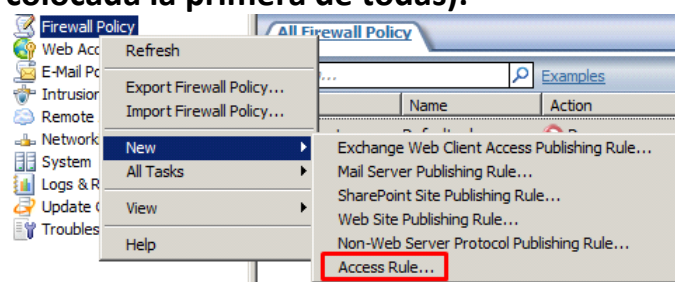
PASO 2 (depende de si está en dominio o workgroup y todo siguiente):

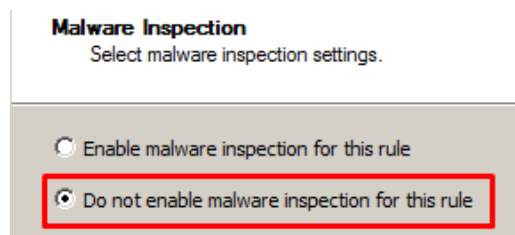


PASO 3 (no usamos microsoft update service y todo no):

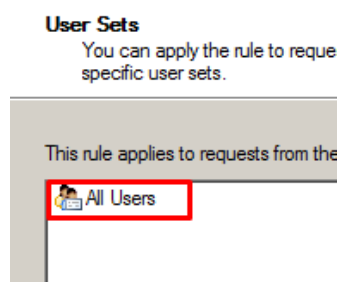
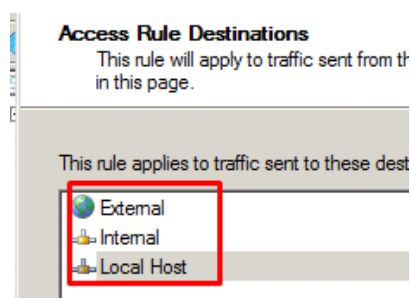
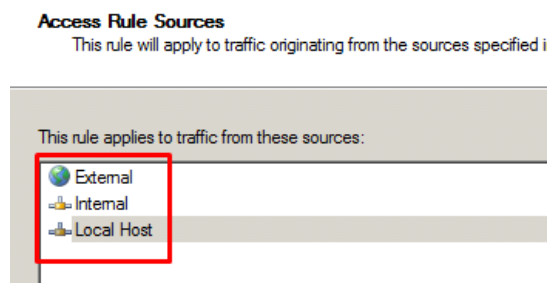


Primera regla, Habilitar todo para comprobar que el firewall funciona ya que por defecto bloquea todas las salidas (siempre tiene que estar colocada la primera de todas):

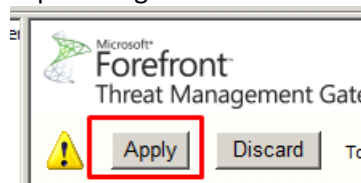




-Añadimos las 3 tanto en el origen como en el destino , ya que queremos permitir todo el tráfico y a todos los usuarios:



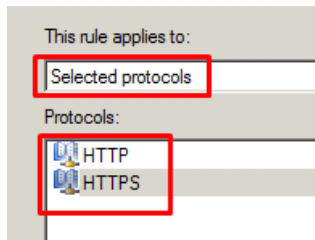
-Aplicar regla:



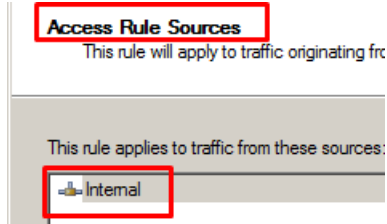
Crear regla para permitir salir a internet:

-Primero deshabilitamos la regla de permitir todo.

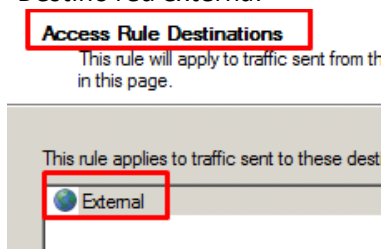
-Seleccionamos protocolo http y https:



-Origen red interna:

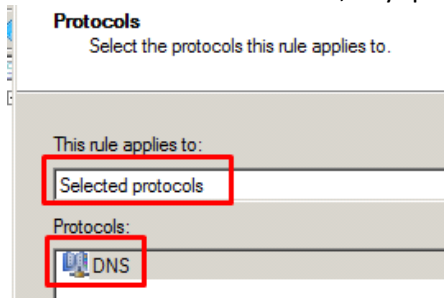


-Destino red externa:



Permitimos tráfico DNS:

-Si tuviéramos el rol de DNS, hay que marcar DNS Server:



-Origen interna

-Destino externo

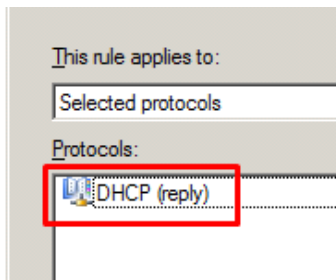
-Aplicamos regla

-No importa el orden de las reglas entre permitir tráfico a internet y permitir DNS, pero siempre tienen que estar debajo de la regla de abrir todo.

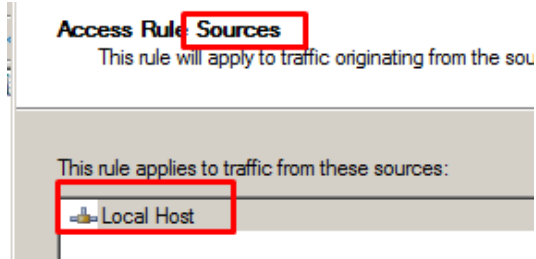
Permitir servicio DHCP a los clientes:

Creamos dos reglas, una para el DHCP Server y otra para el DHCP client:

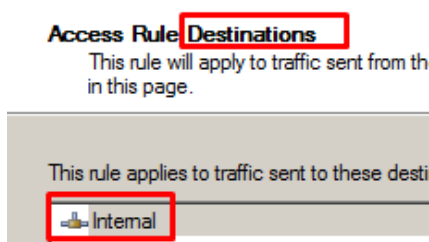
-DHCP Server:



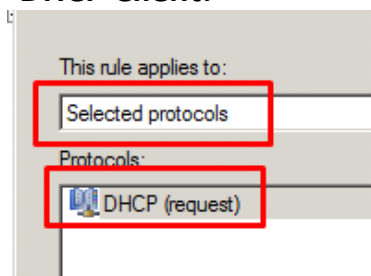
-Origen Local Host



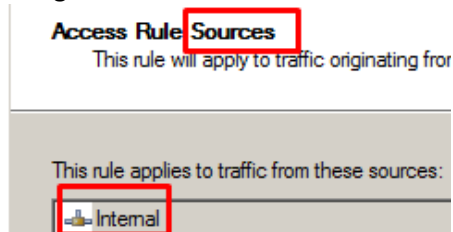
-Destino Interna



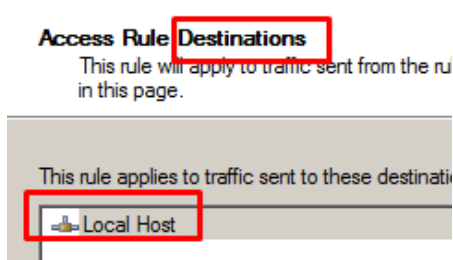
-DHCP Client:



-Origen interna



Destino LocalHost



Aplicamos

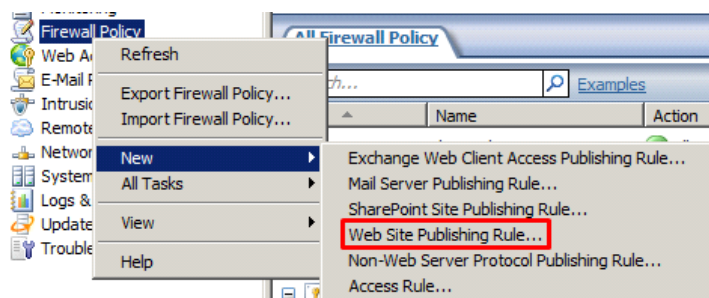
Da igual el orden entre las reglas DHCP Server y DHCP Client

Distinguir un equipo de otro para aplicar reglas:

- Bloquemos al cliente W11-1 la salida a internet.
- Creamos un usuario en el origen de la regla, especificando la IP que queremos que no salga a internet.
- Destino Red Externa.
- Importante que esté encima de la regla de permitir todo el tráfico a internet, ya que si está debajo se cumpliría la de permitir todo el tráfico.

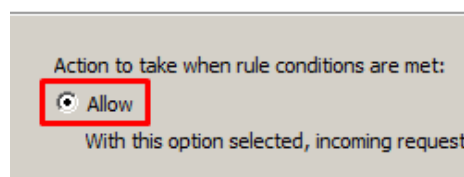
Order	Name	Action	Protocols	From / Listener	To	Condition	Description	Policy
1	Abrir todo	Allow	All Outbound ...	External Internal Local Host	External Internal Local Host	All Users		Array
2	Bloquear internet en W11-1	Deny	HTTP HTTPS	W11-1	External	All Users		Array
3	Permitir salir a internet	Allow	HTTP HTTPS	Internal	External	All Users		Array
4	Permitir DNS	Allow	DNS	Internal	External	All Users		Array
5	Clientes DHCP	Allow	DHCP (request)	Internal	Local Host	All Users		Array
6	Server DHCP	Allow	DHCP (reply)	Local Host	Internal	All Users		Array
Last	Default rule	Deny	All Traffic	All Networks (...)	All Networks (...)	All Users	Predefined acces...	Array

Salir a una página web del servidor IIS de la red11, a través del firewall (red4), estando el cliente en la red del firewall (red4):



Select Rule Action

Specify how you want this rule to respond



Publishing Type

Select if this rule will publish a single Web site or external load balance server farm, or multiple Web sites.

☒ Publish a single Web site or load balancer

Use this option to publish a single Web site, or to publish a load balanced server farm.

Help about [publishing a single Web site or load balancer](#)

☐ Publish a server farm of load balanced Web servers

Server Connection Security

Choose the type of connections Forefront TMG will establish with the published Web server or server farm.

☐ Use SSL to connect to the published Web server or server farm

Forefront TMG will connect to the published Web server or server farm using HTTPS (recommended).

☒ Use non-secured connections to connect the published Web server or server farm

Forefront TMG will connect to the published Web server or

Internal site name:

ws1

The internal site name is the name of the Web site you are publishing as it appears in a browser. Typically, this is the name internal users type into their browsers to reach the Web site.

If Forefront TMG cannot resolve the internal site name, Forefront TMG can connect to the published server by using the computer name or IP address of the server hosting the site.

☒ Use a computer name or IP address to connect to the published server

DIRECCIÓN SERVIDOR IIS

Computer name or IP address:

192.168.11.103

Public Name Details

Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for:

Any domain name

Incoming Web requests will be forwarded to the published Web site without the domain name.

Web listener:

IIS

Listener properties:

Property	Value
Description	
Networks	External
Port(HTTP)	80


Aplicar


Desde un cliente accedemos con la IP del firewall de la red4, y comprobamos que llega al servidor de la red11.

Configurar forefront con 3 adaptadores y salir a través del firewall, para acceder al servidor IIS alojado en la red DMZ:

-Añadimos nuevo adaptador DMZ.

Roles Configuration

 **Launch** Getting Started Wizard

 **Configure network settings**
Define network settings for Forefront TMG, including IP settings, routing rules, and network relationships.

Getting Started - Network Setup Wizard

Network Template Selection
Select the network template that best fits your network topology.

☐ Edge firewall
☒ 3-Leg perimeter
☐ Back firewall

VPN Clients Network
External Network

Network adapter connected to the perimeter network:
DMZ

IP address: 192 . 168 . 80 . 1
Subnet mask: 255 . 255 . 255 . 0
DNS server: . . .

What type of IP addresses do servers in the Perimeter network use?
☐ Public. There is a NAT relationship between the Perimeter network and Internal network, and a route relationship between the Perimeter network and External network.
☒ Private. There is a route relationship between the Perimeter network and the Internal network, and NAT relationship between the Perimeter network and External network.

Hacemos lo mismo que en el anterior paso, pero cambiando la IP al configurar la regla por la del servidor (que contiene la página web) que está alojado ahora en la red DMZ. Cambiarlo tanto en la regla del firewall como en la configuración del servidor IIS. Al crear el listener, que sea la externa.