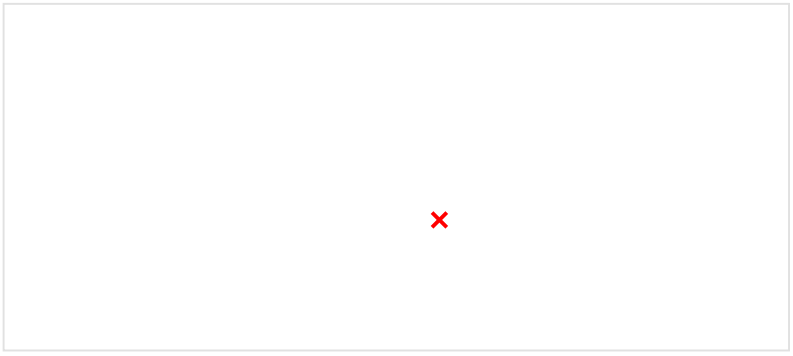
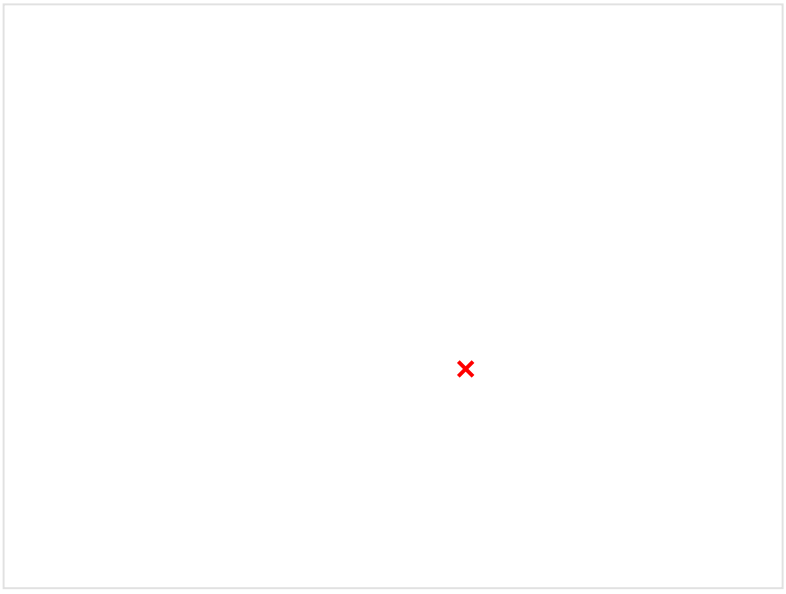
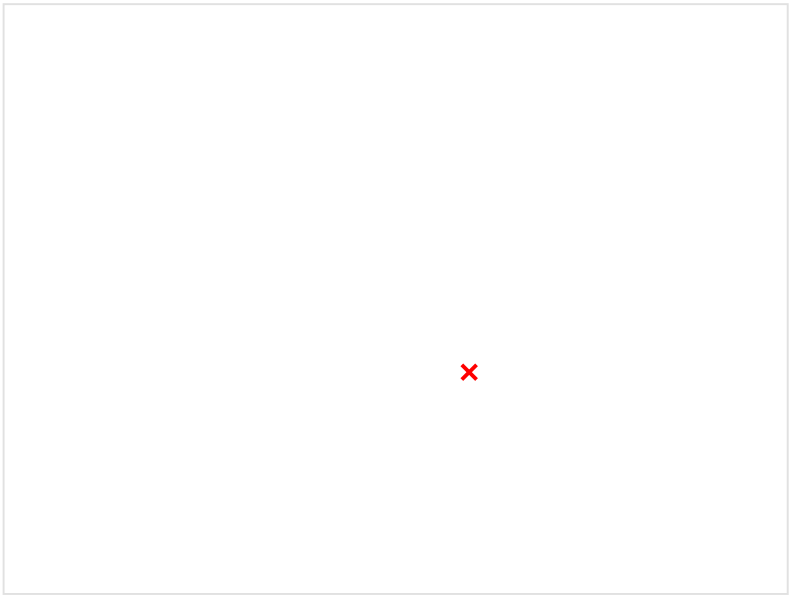
Forefront (firewall)

martes, 17 de octubre de 2023 9:04

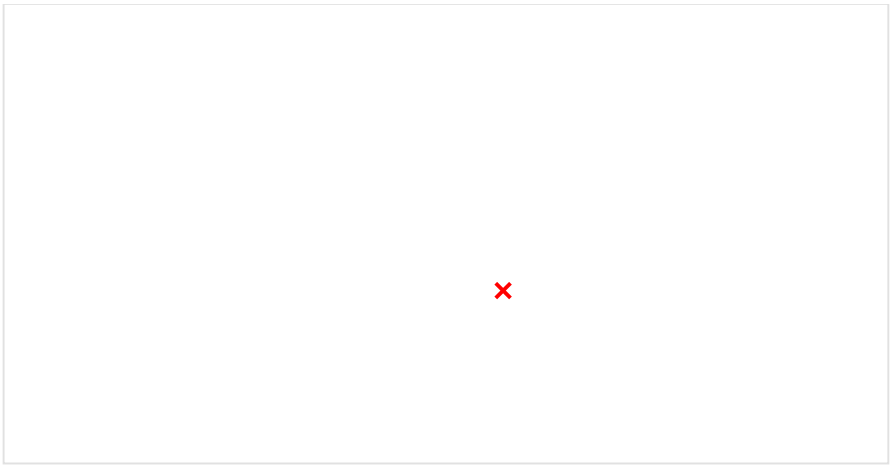
Ejecutamos la aplicación:



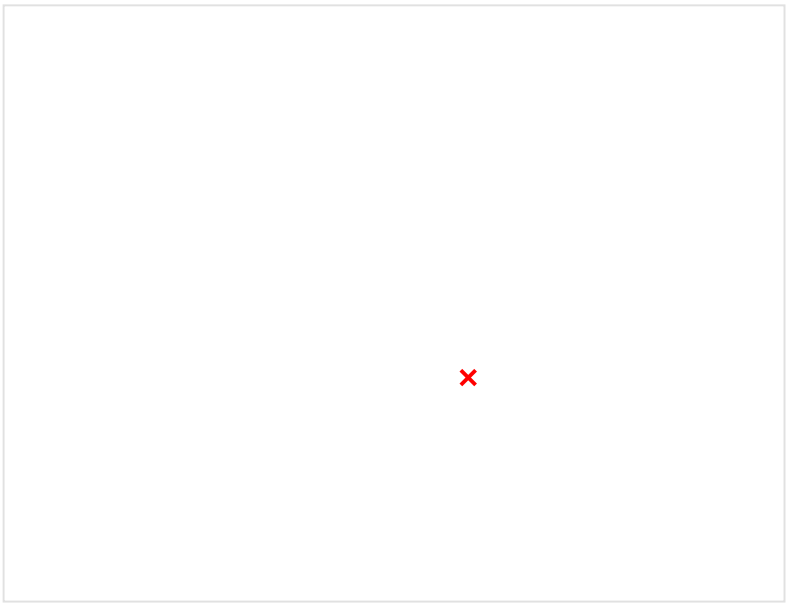




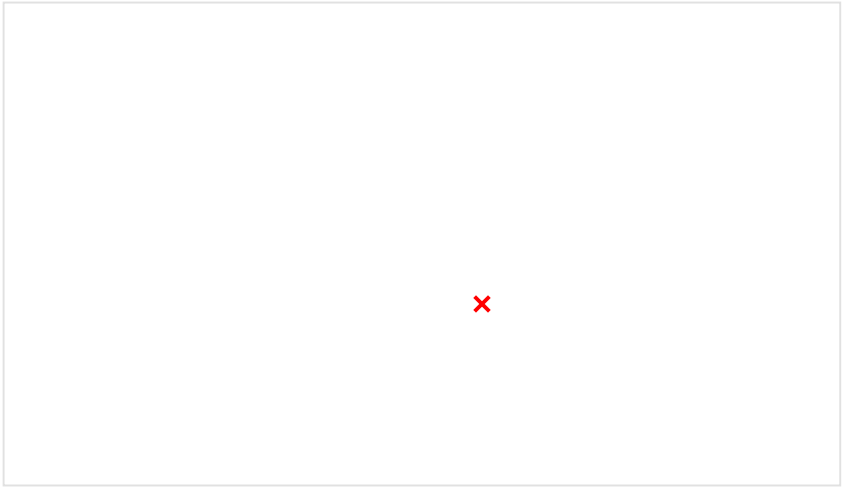
Aquí tenemos que meter el adaptador de la red interna



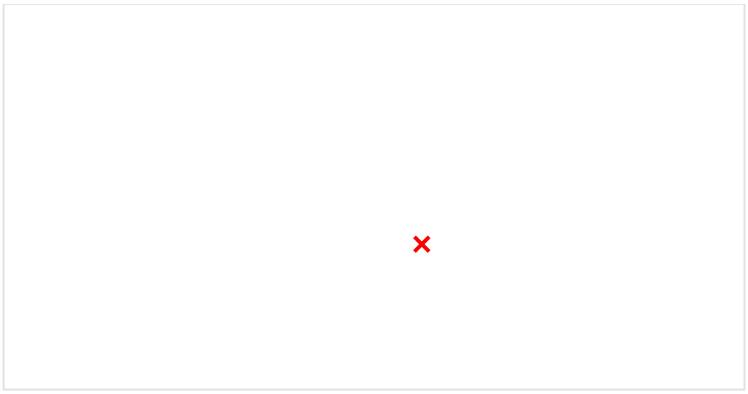
No marcar este cuadrado



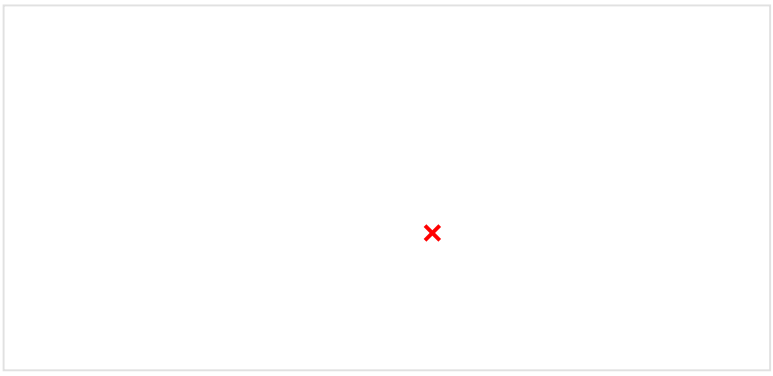
Después de la instalación ejecutar este programa y todo para adelante



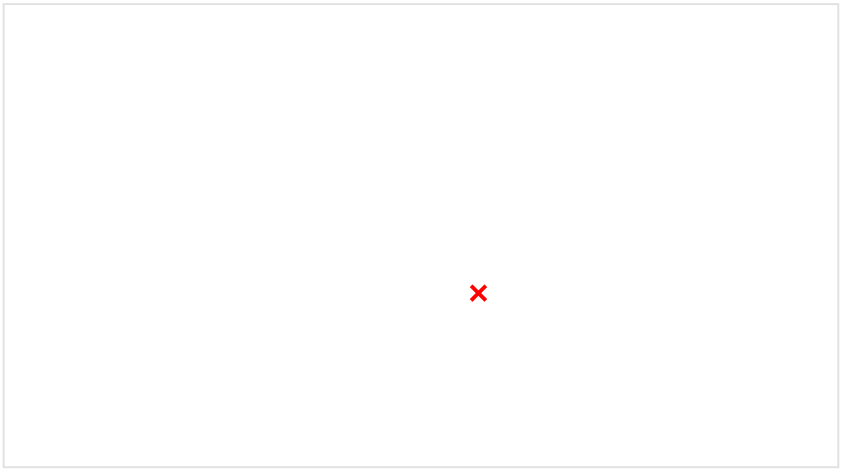
Después instalamos el update 1



Y por último el 2



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

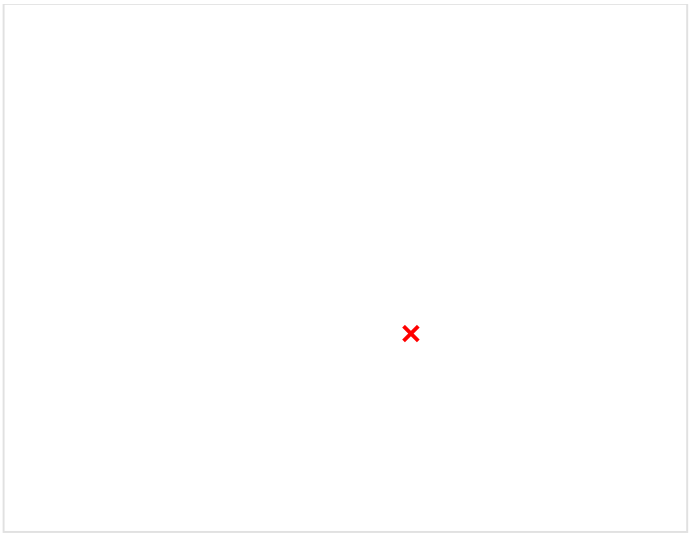


Anclamos al inicio el programa forefront y borramos las carpetas

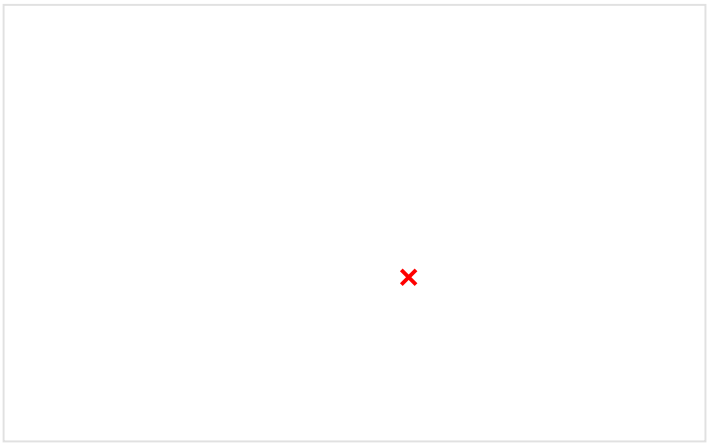
---

-Configurar forefront:

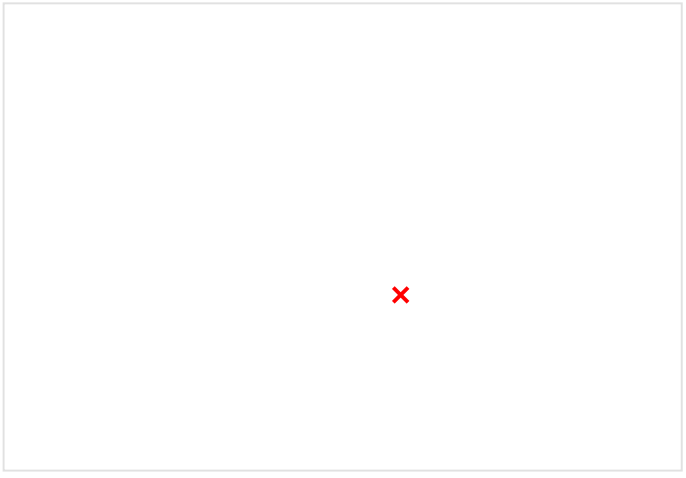
Paso 1:



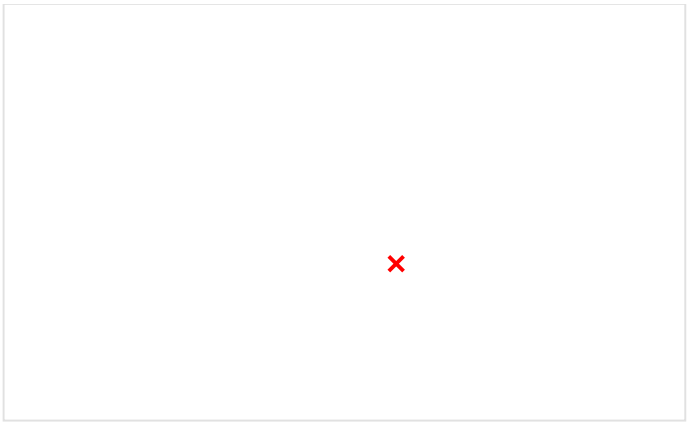
-Red interna:



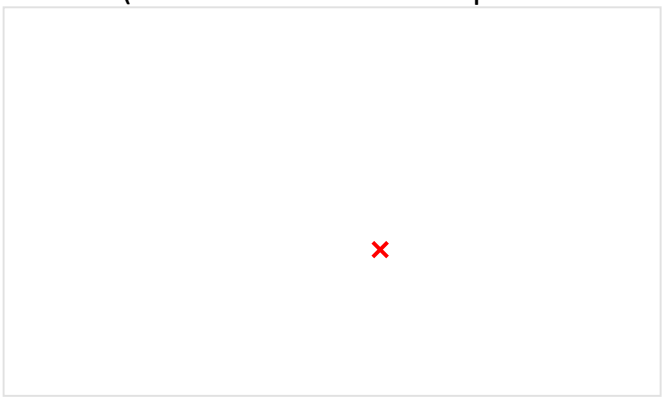
-Red externa:



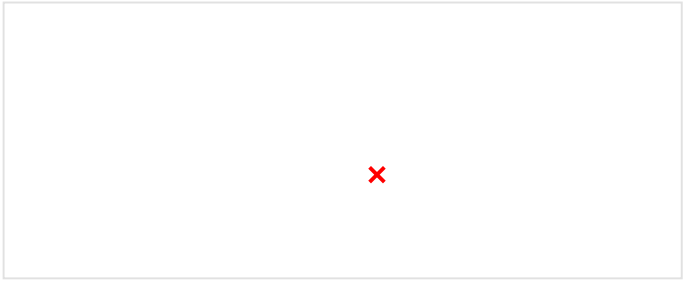
PASO 2 (depende de si está en dominio o workgroup y todo siguiente):

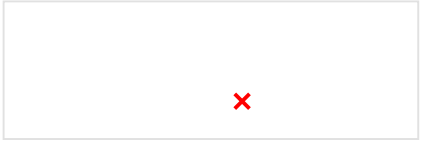


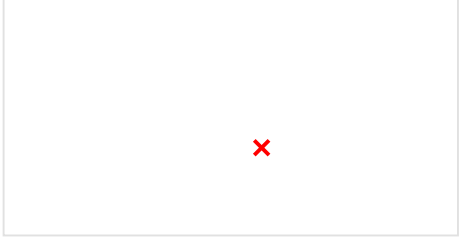
PASO 3 (no usamos microsoft update service y todo no):

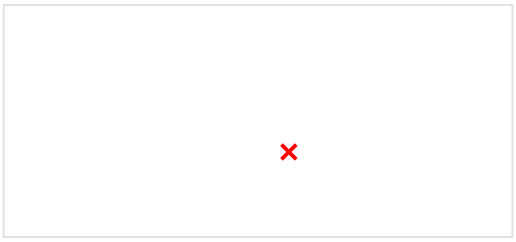


Primera regla, Habilitar todo para comprobar que el firewall funciona ya que por defecto bloquea todas las salidas (siempre tiene que estar colocada la primera de todas):

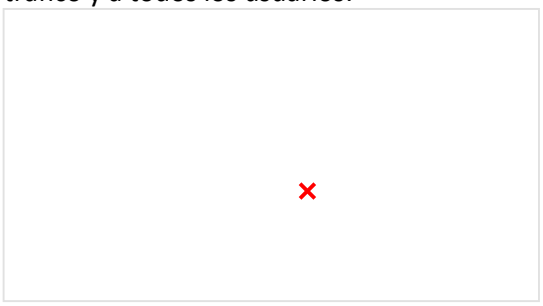


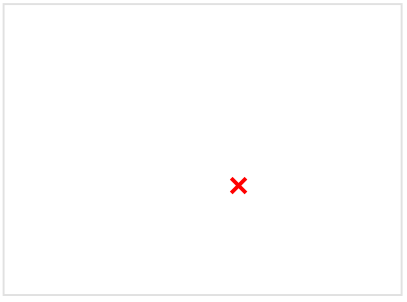


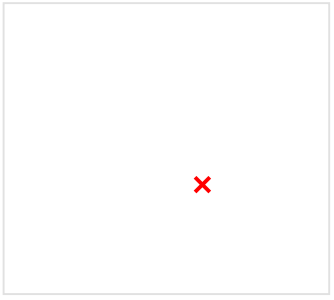




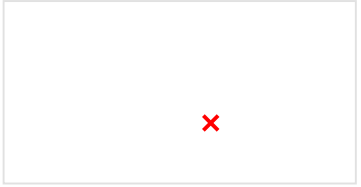
-Añadimos las 3 tanto en el origen como en el destino , ya que queremos permitir todo el tráfico y a todos los usuarios:





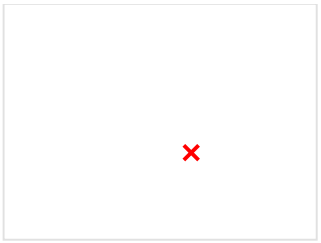


-Aplicar regla:

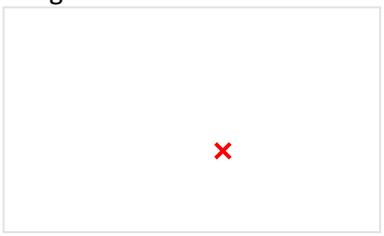


Crear regla para permitir salir a internet:
-Primero deshabilitamos la regla de permitir todo.

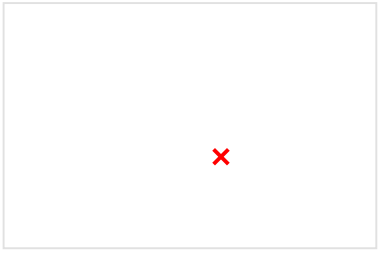
-Seleccionamos protocolo http y https:



-Origen red interna:

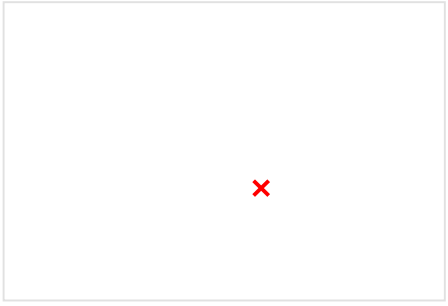


-Destino red externa:



Permitimos tráfico DNS:

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

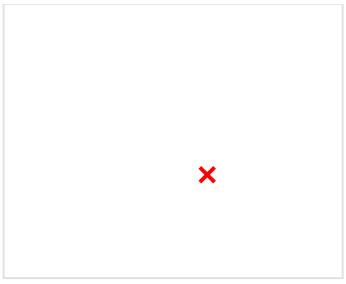


-Origen interna
-Destino externo
-Aplicamos regla
-No importa el orden de las regla entre permitir tráfico a internet y permitir DNS, pero siempre tienen que estar debajo de la regla de abrir todo.

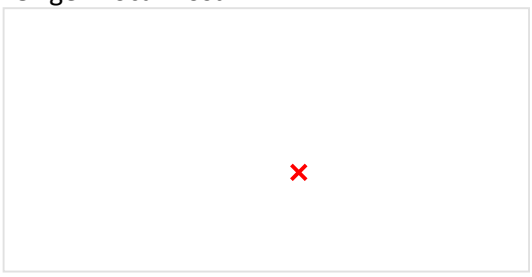
Permitir servicio DHCP a los clientes:

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

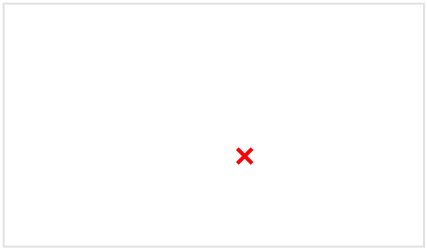
-DHCP Server:



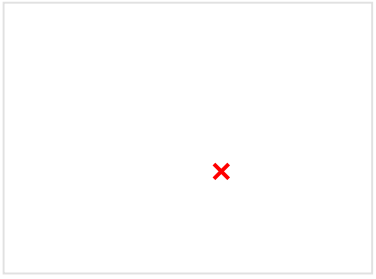
-Origen Local Host



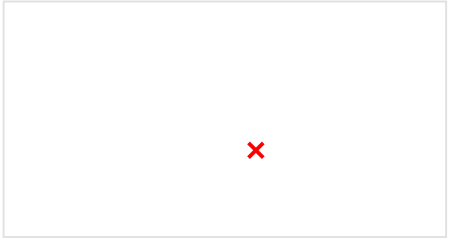
-Destino Interna



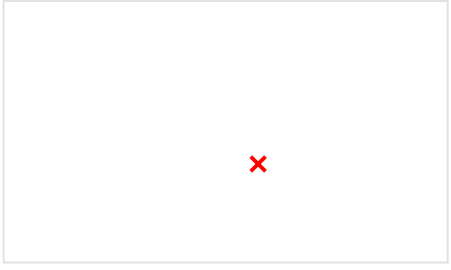
-DHCP Client:



-Origen interna



Destino LocalHost

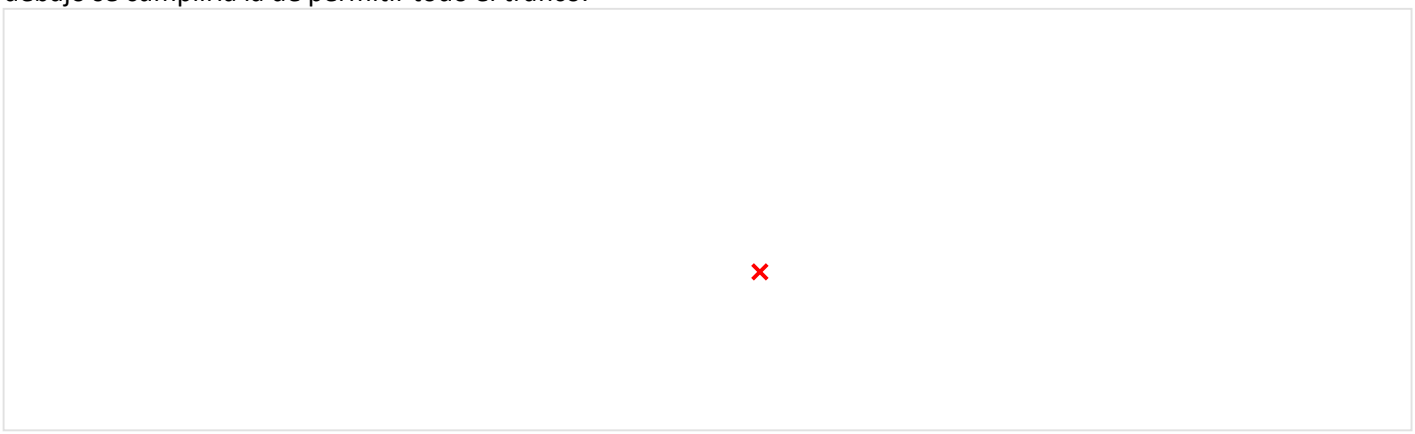


Aplicamos

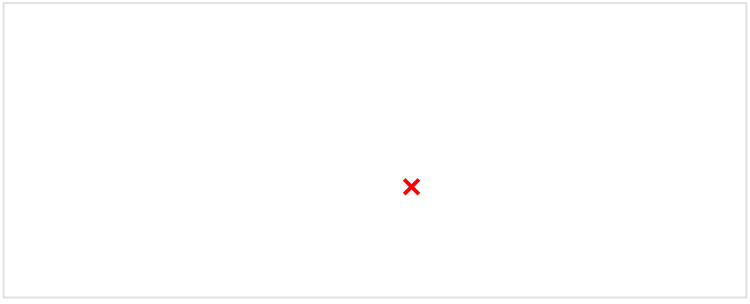
Da igual el orden entre las reglas DHCP Server y DHCP Client

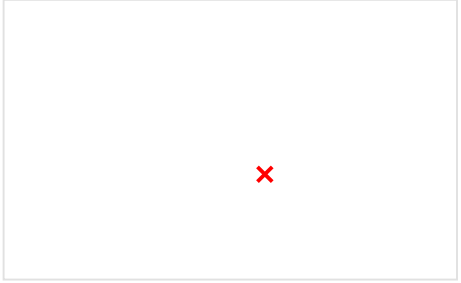
Distinguir un equipo de otro para aplicar reglas:

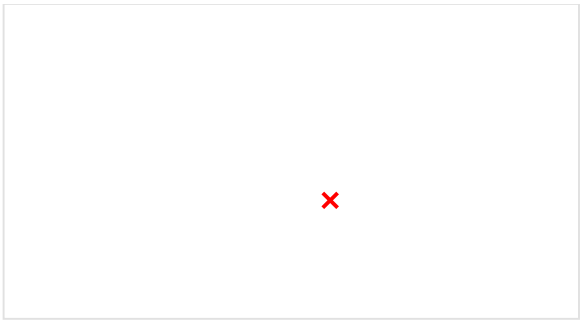
-Bloquemos al cliente W11-1 la salida a internet.
-Creamos un usuario en el origen de la regla, especificando la IP que queremos que no salga a internet.
-Destino Red Externa.
-Importante que esté encima de la regla de permitir todo el tráfico a internet, ya que si está debajo se cumpliría la de permitir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

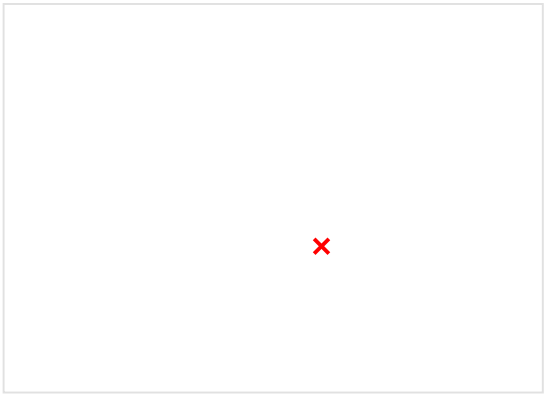


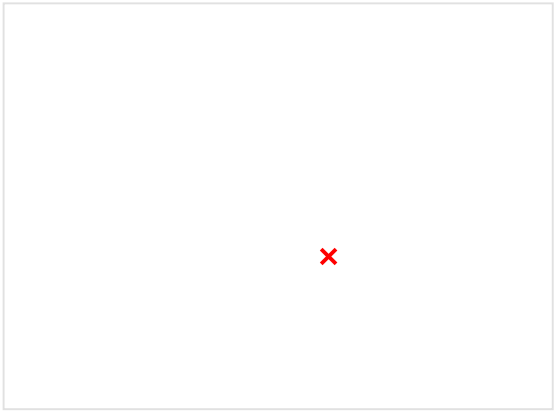
Salir a una página web del servidor IIS de la red11, a través del firewall (red4), estando el cliente en la red del firewall (red4):

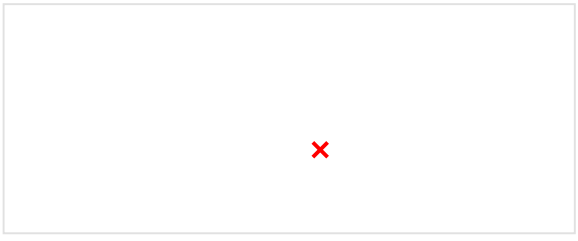


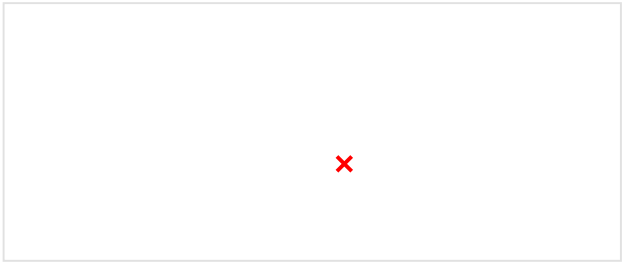










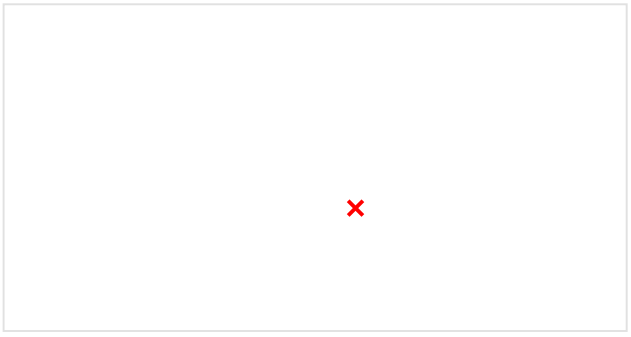


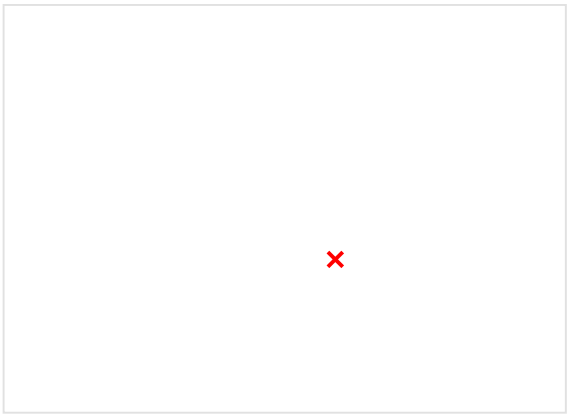
Aplicar

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.





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.