ACTIVIDAD 2 - FIREWALL MIKROTIK

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

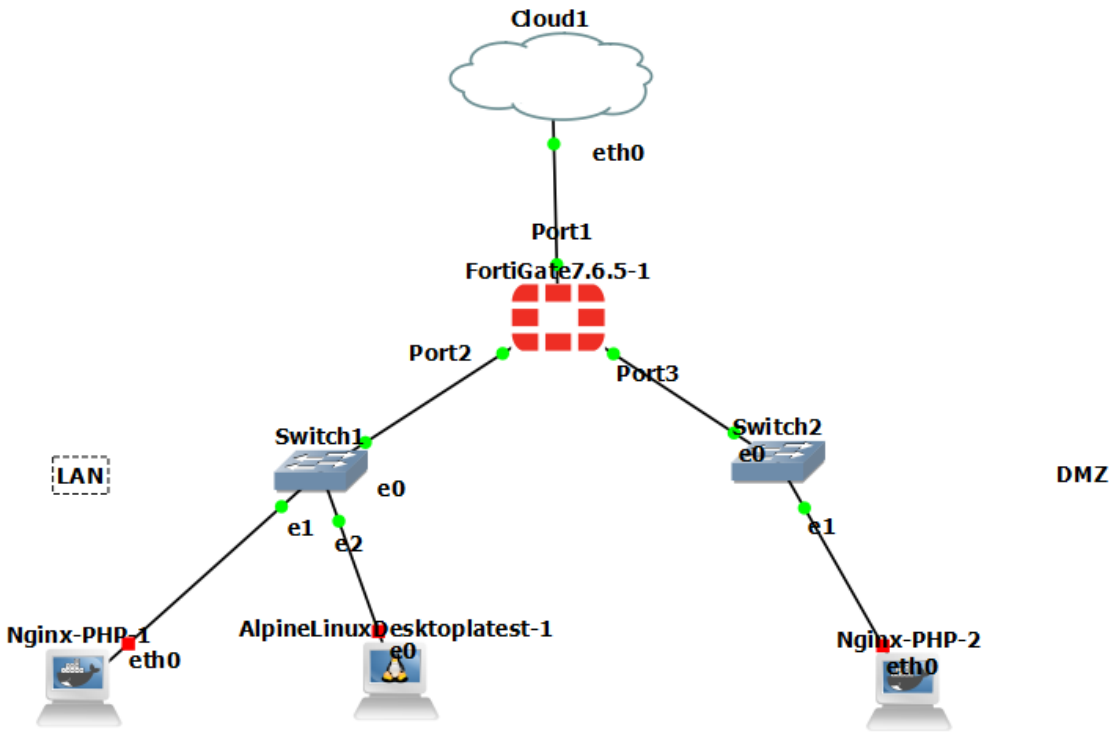
Diagrama en servidor GNS3 del Instituto: CSA_Actividad_2-Firewall Fortigate

Índice

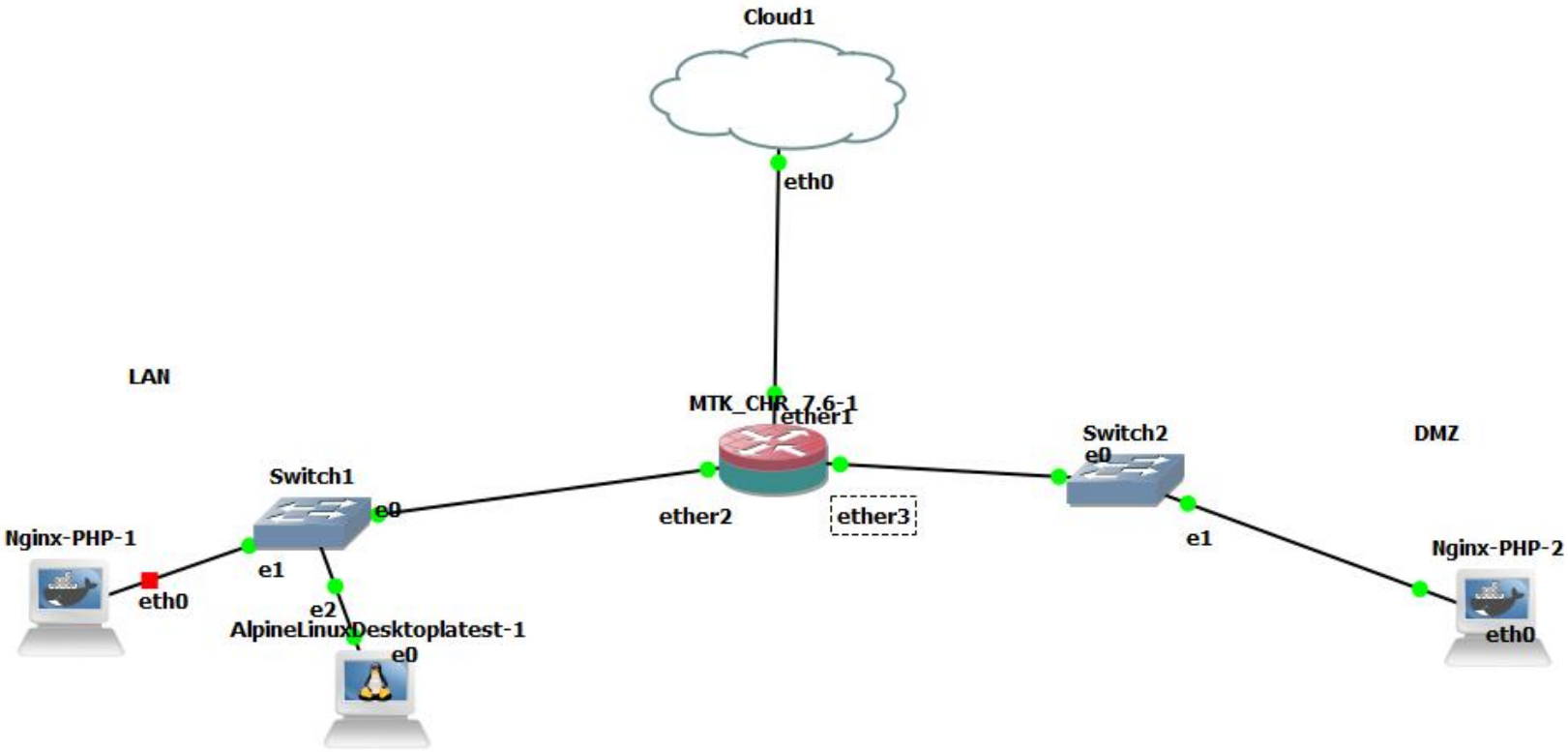
1. Escenario y Topología

El objetivo es configurar un clúster de seguridad para la empresa "CorpNet". La red se divide en tres zonas:

- **WAN (Port1):** Conexión a Internet (Simulada con nodo Cloud).
- **LAN (Port2):** Usuario interno y un servidor de web interno.
- **DMZ (Port3):** Servidor Web público.



Ante la imposibilidad de usar un equipo Fortigate en GNS3 por problemas de licencia, usamos un router Mikrotik.

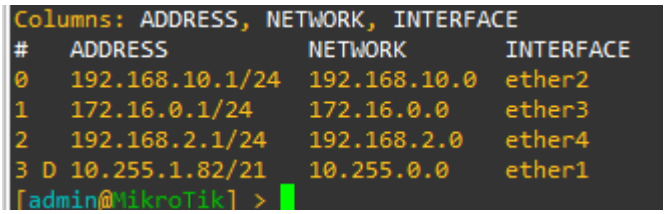


2. Acceso a Mikrotik

Acceder a la interfaz web de Mikrotik desde el navegador local de tu equipo

Para ello debemos saber cual es la IP de la interfaz del router Mikrotik que da acceso a Internet:

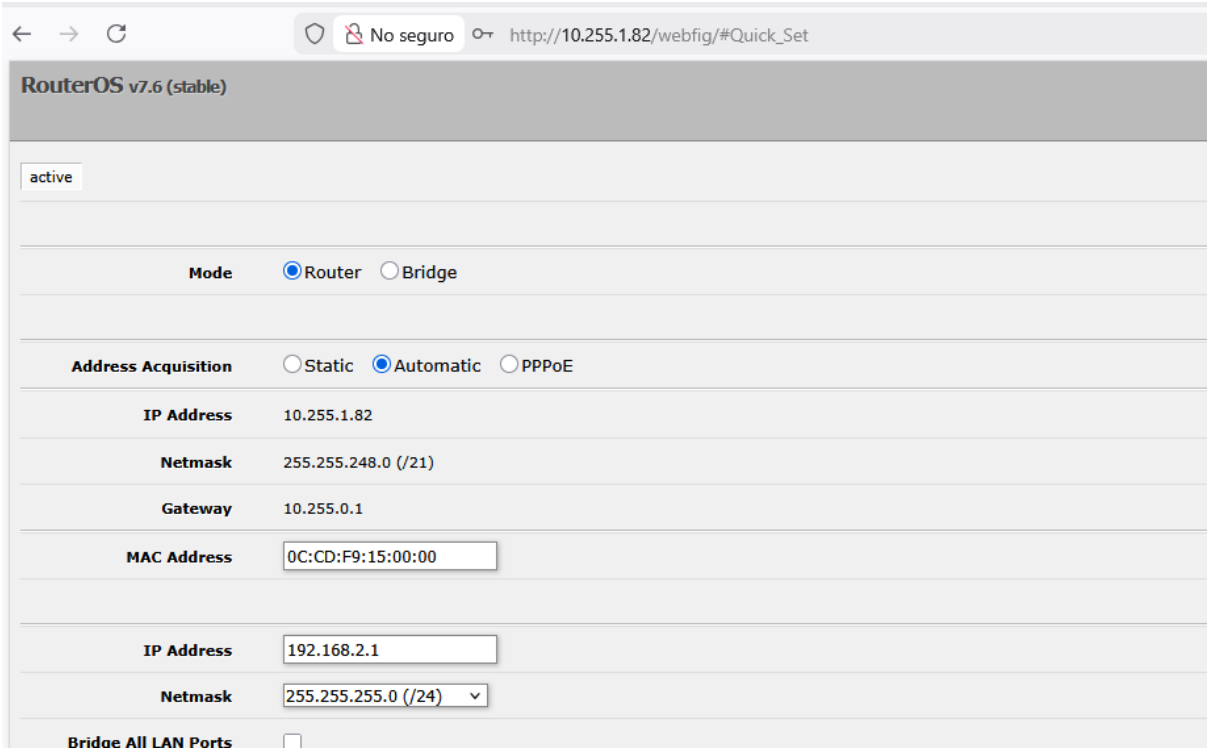
Accedemos a la terminal del router y hacemos: ip address/print



En nuestro caso es el Ethernet1: 10.255.1.82/21

Ponemos en el navegador: http://10.255.1.82/

Metemos las credenciales y listo:



3. Configuración de Red

- **WAN (Port1):** DHCP (proporcionado por el nodo Cloud).
- **LAN (Port2):** `192.168.10.0/24` (IP FortiGate: `.1`).
- **DMZ (Port3):** `172.16.0.0/24` (IP FortiGate: `.1`).

Desde la propia terminal del router Mikrotik se puede realizar la configuración de las IP estáticas.

ip address/add address=192.168.10.1/24 interface=ether2

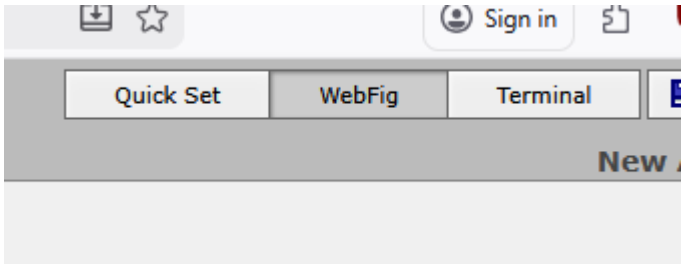
ip address/add address=172.16.0.1/24 interface=ether3

Para ver las ips asignadas: **ip address/print**

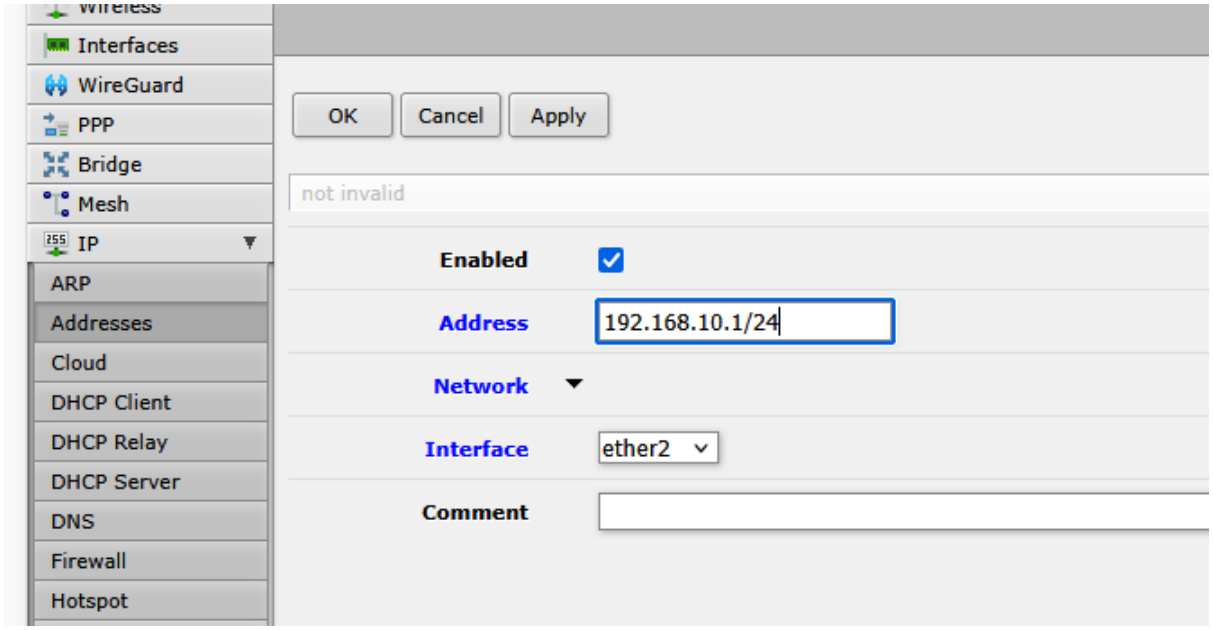
Quitar IP: **ip address/remove 4 (o el número que sea)**

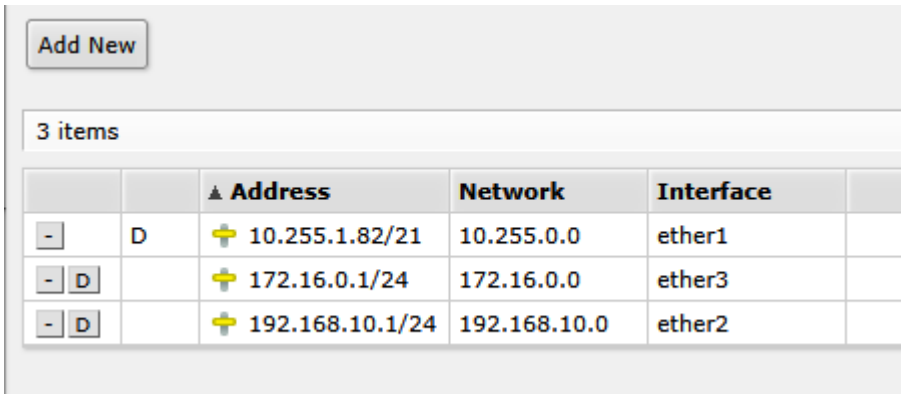
```
[admin@MikroTik] > ip address/print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS           NETWORK       INTERFACE
0   192.168.10.1/24   192.168.10.0  ether2
1   172.16.0.1/24     172.16.0.0    ether3
2 D 10.255.1.82/21    10.255.0.0    ether1
[admin@MikroTik] >
```

Desde el navegador: en la parte derecha, seleccionamos "**Webfig**".



Luego IP → Addresses: Indica IP y Máscara de Red y la interfaz del router.





4: Implementación de Cortafuegos

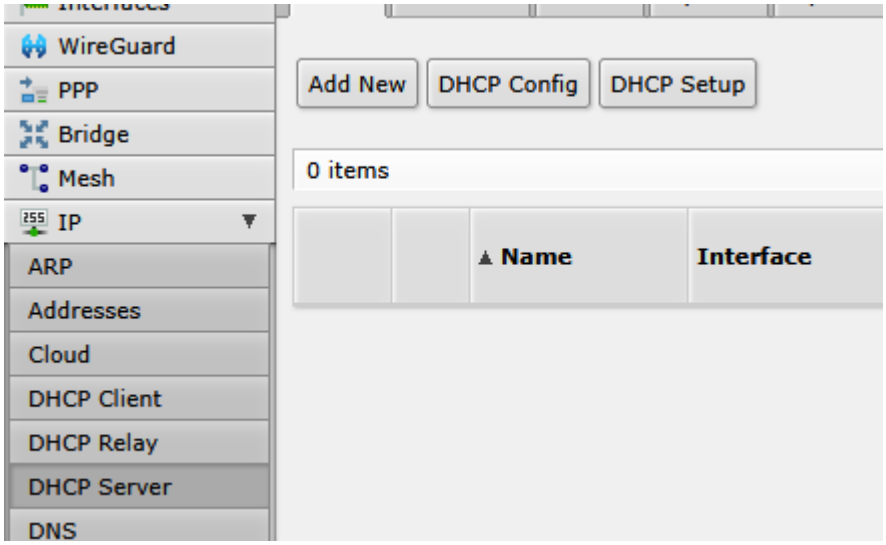
Configurar el Mikrotik desde cero (vía web en el cliente Alpine). Comprueba que funcionan los bloqueos y permisos, y documenta que el acceso es únicamente de la forma esperada.

• Tarea 1: Salida a Internet:

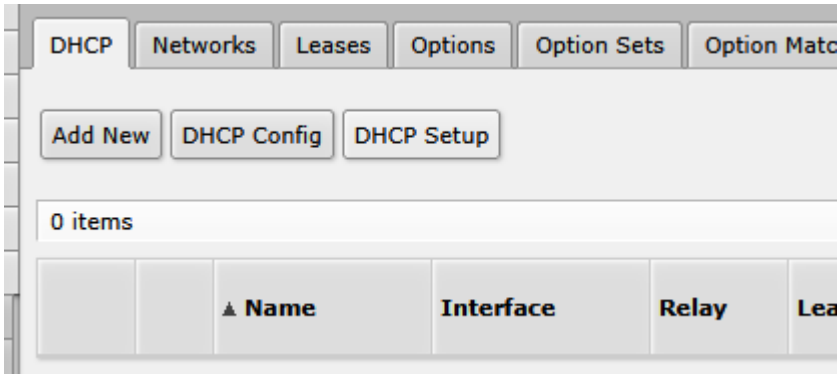
Configurar una política de `LAN -> WAN` con NAT habilitado.

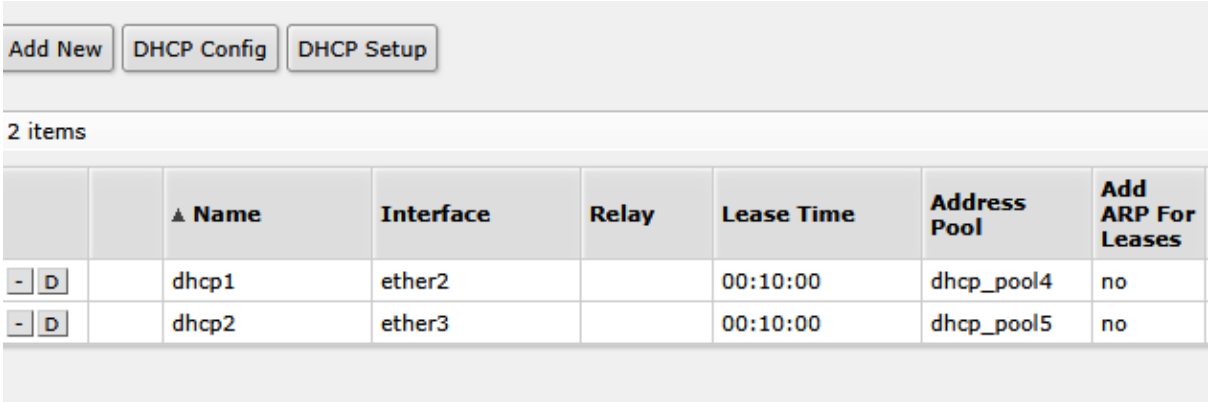
- *Objetivo:* Probar que el cliente navega.

Establecemos servidor DHCP en los puertos (de momento solo el de ethernet2).



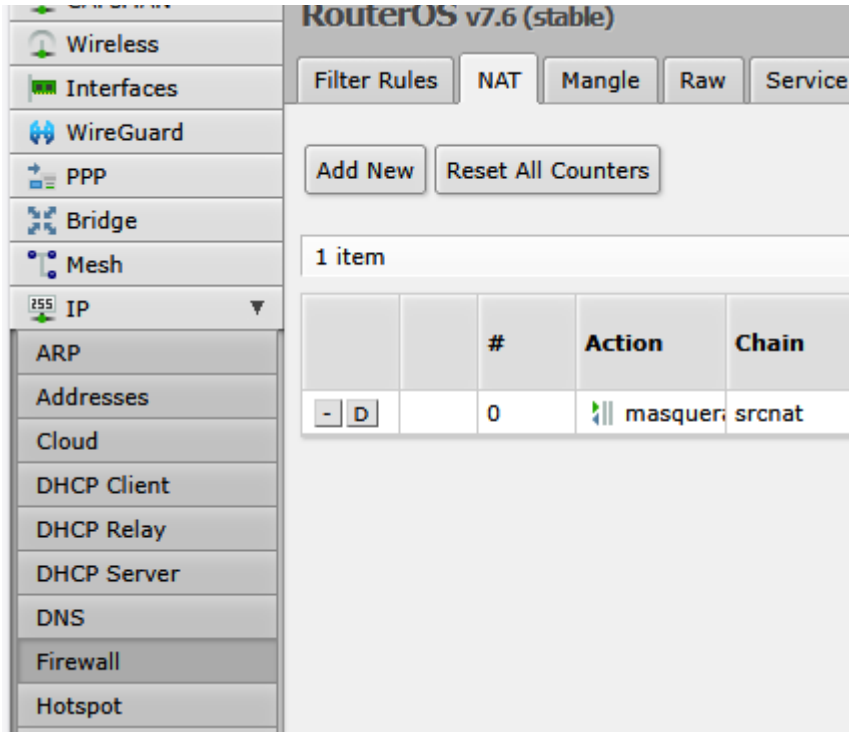
Le damos a DHCP Setup y seguimos el asistente. Una vez que seleccionamos la interfaz solo hay que seguir el asistente.



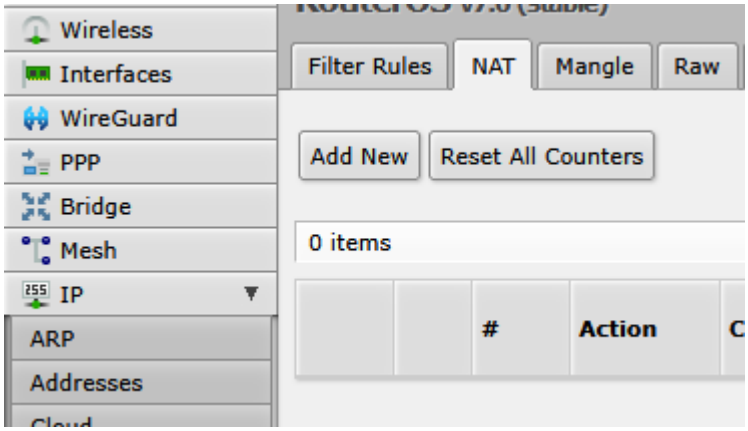


Configuración del NAT.

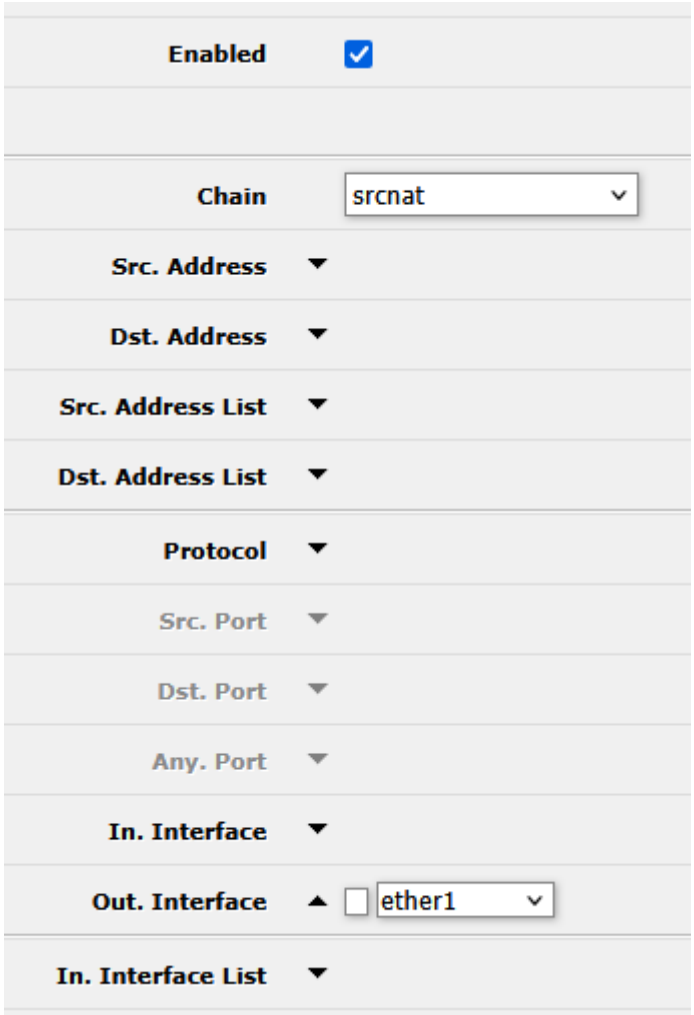
Firewall → NAT



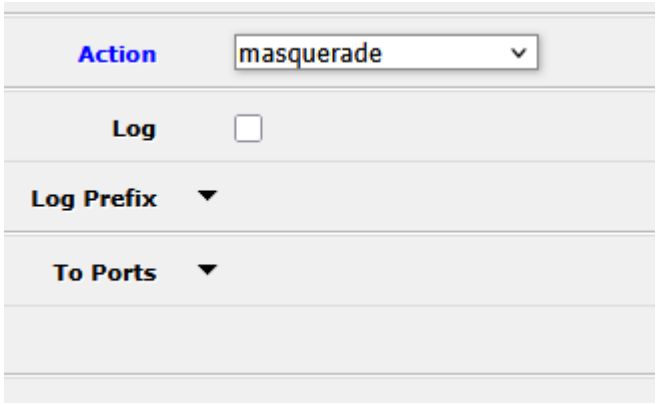
“Add new”



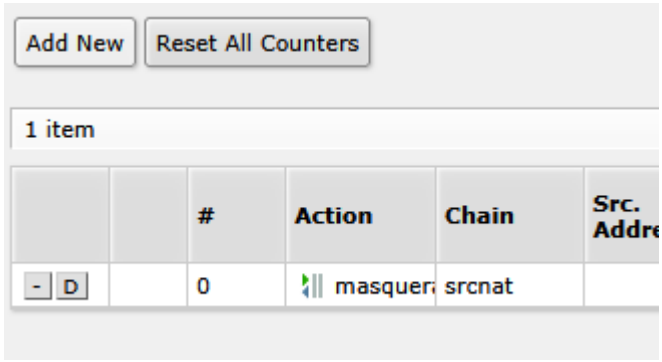
Chain → “srcnat” y la interfaz de salida “all”.



En “Action” → “masquerade”



Guardamos.



Ahora el cliente de la LAN de Ethernet2 tiene acceso a internet.

```
rtt min/avg/max/mdev = 42.776/43.414/43.825/0.395 ms
~ $ ping x.uk
PING x.uk (185.249.71.213) 56(84) bytes of data.
64 bytes from 185.249.71.213: icmp_seq=1 ttl=47 time=45.0 ms
64 bytes from 185.249.71.213: icmp_seq=2 ttl=47 time=44.4 ms
64 bytes from 185.249.71.213: icmp_seq=3 ttl=47 time=43.2 ms
64 bytes from 185.249.71.213: icmp_seq=4 ttl=47 time=42.8 ms
64 bytes from 185.249.71.213: icmp_seq=5 ttl=47 time=42.2 ms
64 bytes from 185.249.71.213: icmp_seq=6 ttl=47 time=42.9 ms
64 bytes from 185.249.71.213: icmp_seq=7 ttl=47 time=42.8 ms
64 bytes from 185.249.71.213: icmp_seq=8 ttl=47 time=44.3 ms
^C
--- x.uk ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7015ms
rtt min/avg/max/mdev = 42.224/43.450/44.972/0.918 ms
~ $
```

- Tarea 2: Publicación de la DMZ (DNAT/VIP).

Crear un Virtual IP para que el servidor `Nginx-PHP-2` (DMZ) sea accesible desde la IP de la WAN usando Port Forwarding al puerto 80.

- *Objetivo:* Acceder a la web de la DMZ desde fuera.

¿Qué es un Virtual IP (VIP)?

Normalmente, el NAT (Source NAT) permite que muchos equipos internos salgan por una sola IP pública. El **Virtual IP es NAT de Destino (DNAT)**: permite que alguien desde fuera escriba la IP de la WAN del FortiGate y sea redirigido automáticamente a la IP privada del servidor en la DMZ.

¿Qué es port forwarding?

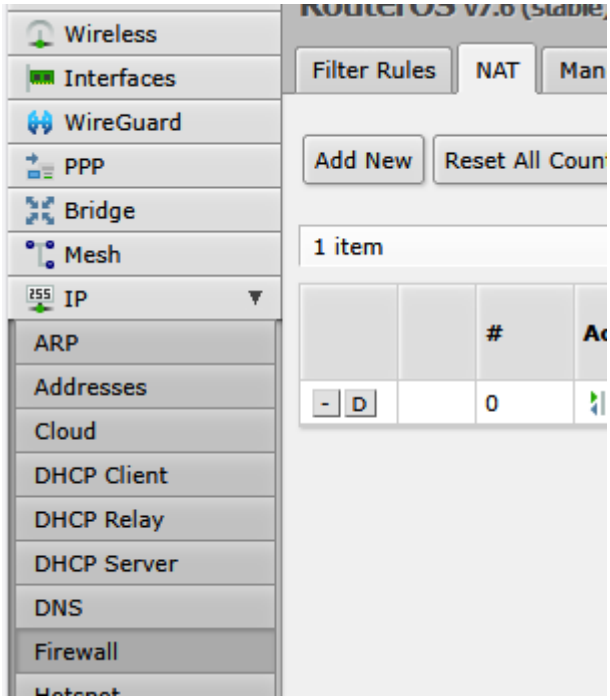
Es una técnica de red que permite que computadoras externas (desde Internet) se conecten a un dispositivo o servicio específico dentro de una red privada (LAN o DMZ) que estará mapeado en un puerto específico.

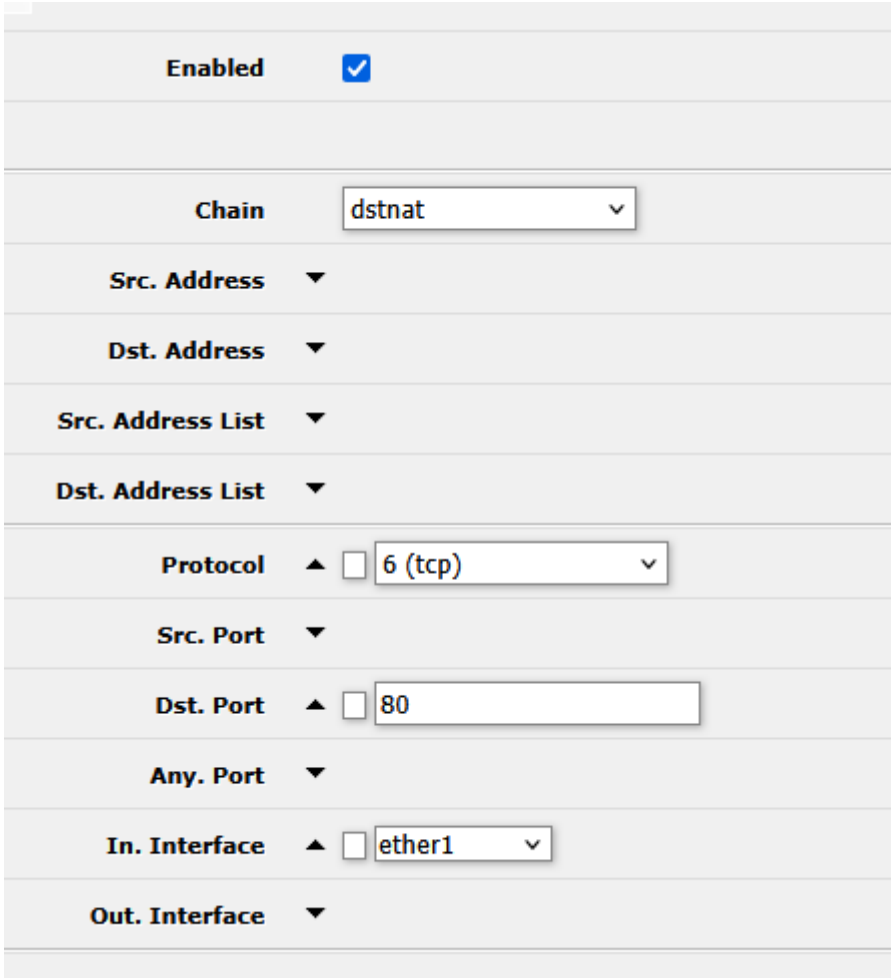
Antes de nada, vamos a fijar la IP del servidor Nginx: Clic derecho en el servidor y le das a “Edit Config”.

```
# Static config for eth0
auto eth0
iface eth0 inet static
                address 172.16.0.50
                netmask 255.255.255.0
                gateway 172.16.0.1
                up echo nameserver 172.16.0.1> /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
#               hostname Nginx-PHP-2
```

Ahora volvemos a la interfaz de Mikrotik.





“Chain”→ dstnat

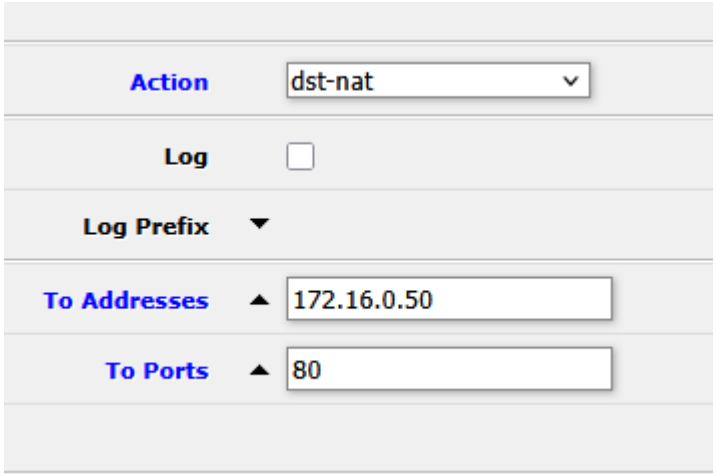
“Dst. Address” → La IP pública del router. En nuestro caso, al estar en laboratorio, no es realmente pública (tendríamos que usar la del Instituto, cosa que no podemos hacer); es la IP que conecta al router con el resto de internet.

“Protocol”: El protocolo que vamos a usar. En nuestro caso “tcp”.

“Dst. Port”: Usamos el puerto 80.

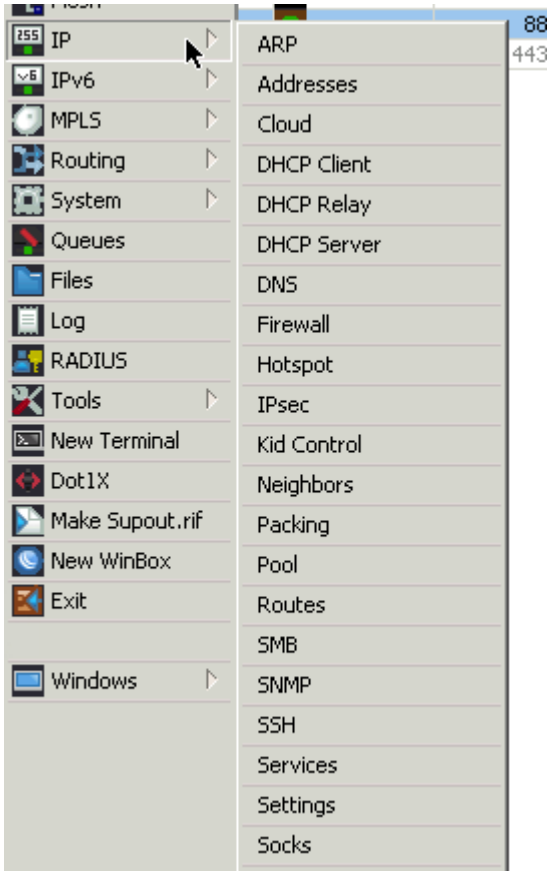
Luego nos vamos a “Action” y debemos seleccionar “dst-nat”.

Indicamos en “To Addresess” la IP del servidor “Nginx-PHP-2” y en “To Ports” el puerto que se usará (80 es el puerto por defecto de los servidores web HTTP).

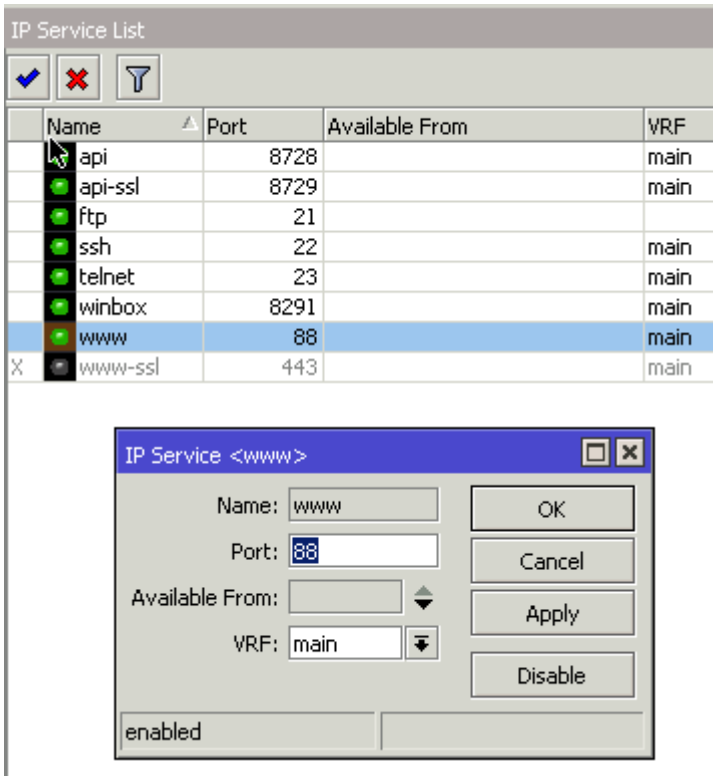


ATENCIÓN: MUY IMPORTANTE: Antes de darle a Apply o a OK y guardar la configuración, ten en cuenta que para acceder a la terminal de Mikrotik desde tu navegador, estas usando la IP “Pública” del router y usas el puerto 80. Si activas la configuración ahora te echará a fuera y no podrás seguir configurando el router desde tu equipo. Para evitar esto, sigue los siguientes pasos:

IP → Services



Establece un puerto diferente para el servicio “www”, por ejemplo, el 88:



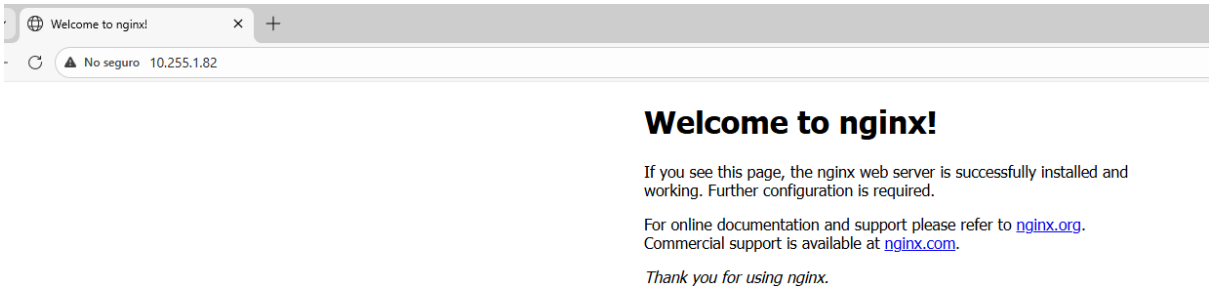
Ahora podrás seguir usando la interfaz desde el navegador de tu equipo, solo que ahora tendrás que poner la IP_Servidor:88 → **10.255.1.82:88**

Si por desgracia has activado la configuración antes de ver esto y estás en GNS3, puedes usar un equipo “webterm-winbox2” y acceder desde el diagrama.

- Volvemos a la parte donde accedemos al servidor Nginx. Para poder acceder a el desde nuestro navegador, solo tenemos que poner la IP pública del router. En este caso:

http://10.255.1.82/

CUIDADO: Puede que se haya guardado en la caché del navegador los datos de la interfaz de Mikrotik y no nos cargue la página del servidor. Usa otro navegador o limpia la cache.



• Tarea 3: Filtrado de Aplicaciones.

Crear un perfil de **Application Control** en la política de la LAN para bloquear "YouTube", permitiendo el resto.

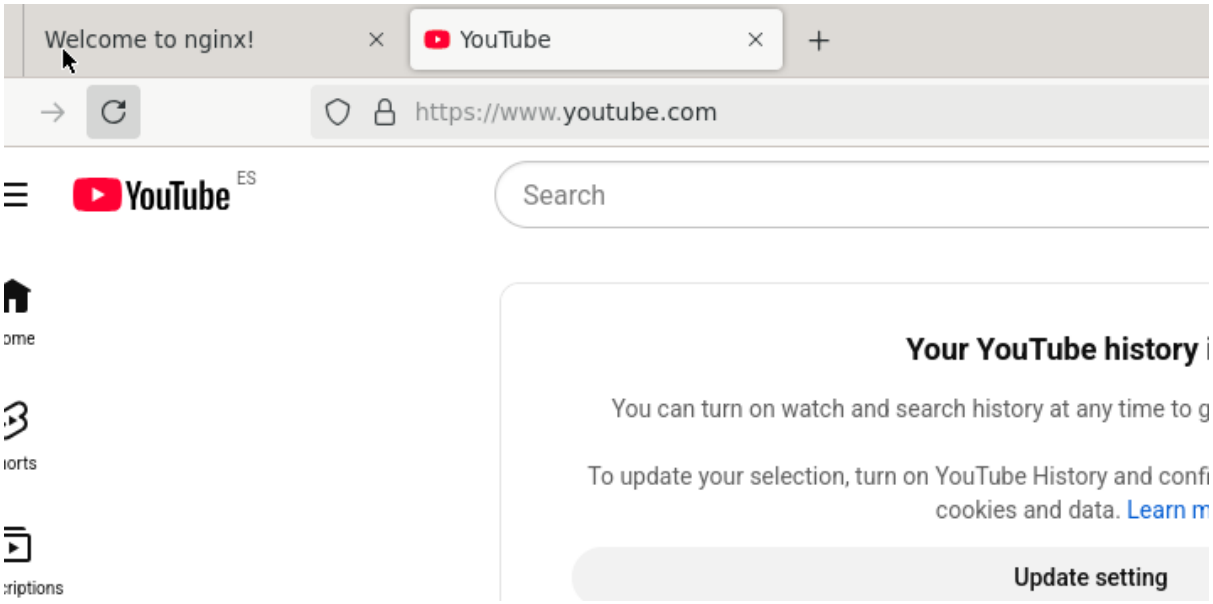
¿Por qué no basta con bloquear la IP?

YouTube tiene miles de direcciones IP y cambian constantemente. Además, comparte infraestructura con Google. Intentar bloquearlo por IP es imposible. El **Control de Aplicaciones** utiliza "firmas" (huellas digitales) para identificar el tráfico de YouTube basándose en el comportamiento de los paquetes, sin importar su IP.

Es una de las diferencias entre un cortafuegos tradicional (que solo ve IPs y puertos) y un **Cortafuegos de Nueva Generación (NGFW)**, que es capaz de "leer" qué aplicación se está usando.

Antes de nada, desde el equipo cliente que está dentro del diagrama comprobamos que hay acceso a Youtube:

```
~ $ ping youtube.com
PING youtube.com (142.250.200.110) 56(84) bytes of data.
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=1 ttl=113 time=49.5 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=2 ttl=113 time=71.7 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=3 ttl=113 time=65.9 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=4 ttl=113 time=14.2 ms
^C
--- youtube.com ping statistics ---
```



Podemos hacer los siguientes pasos con comandos desde la terminal de Mikrotik:

- **Bloquear usando TLS Host / SIN**

Crear regla en firewall

/ip firewall filter

add chain=forward protocol=tcp dst-port=443 tls-host=*.youtube.com action=drop comment="Bloquear YouTube"

add chain=forward protocol=tcp dst-port=443 tls-host=*.googlevideo.com action=drop comment="Bloquear GoogleVideo"

- **Usar Address-List dinámica**

Marcas los dominios:

ip firewall address-list

add list=youtube address=youtube.com

add list=youtube address=googlevideo.com

add list=youtube address=ytimg.com

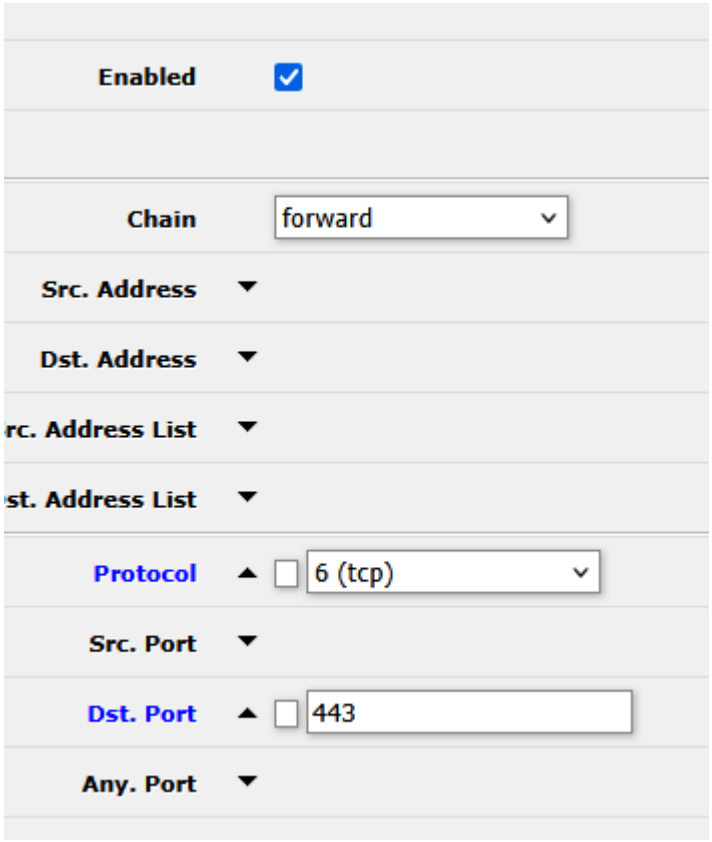
Bloquear tráfico:

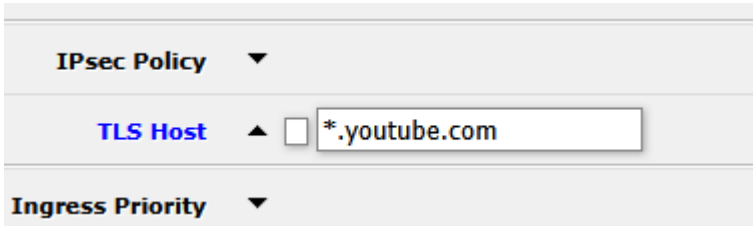
/ip firewall filter

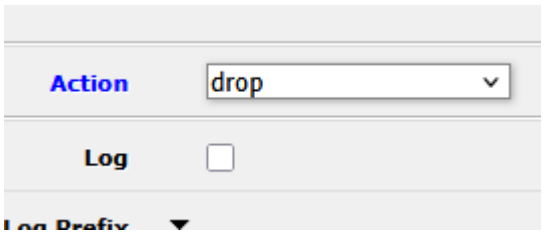
add chain=forward dst-address-list=youtube action=drop comment="Bloquear YouTube completo"

Ahora el método desde la interfaz de Mikrotik:

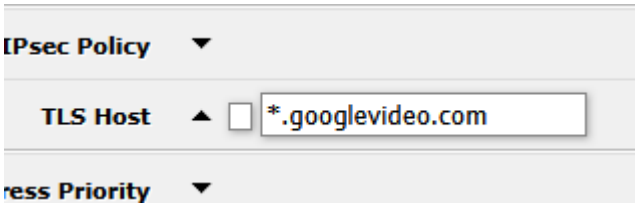
- **Bloquear usando TLS Host / SIN:**



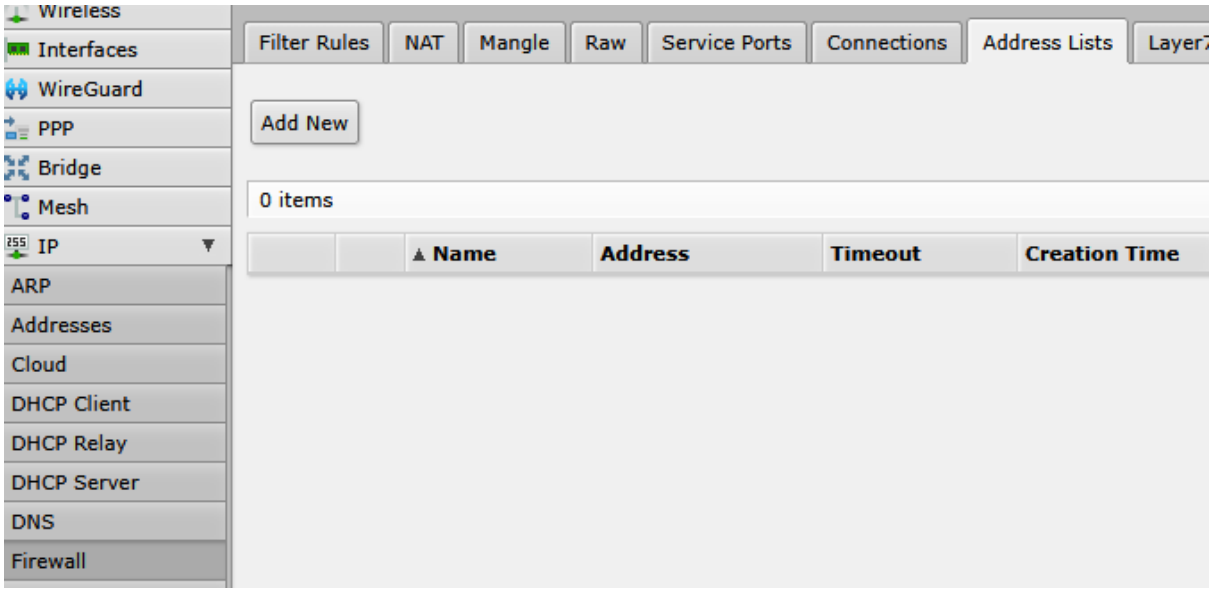


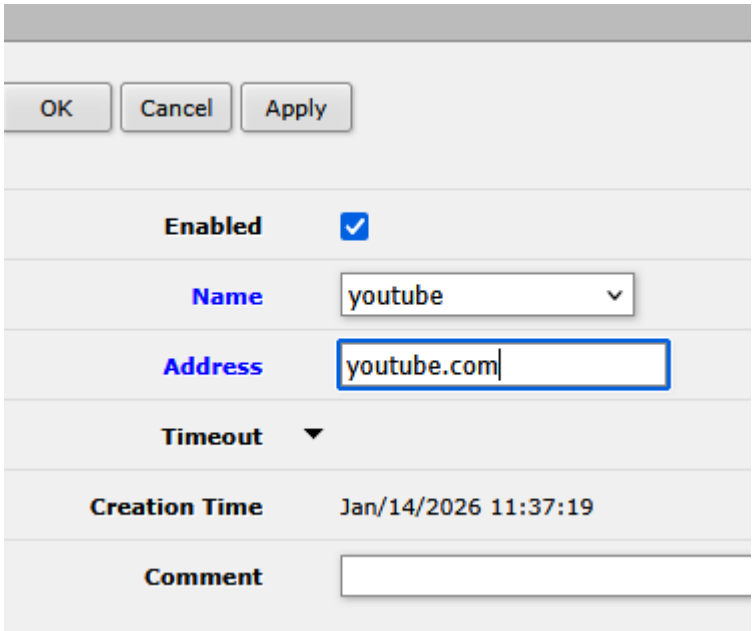


Ahora hacemos lo mismo, pero para “googlevideo.com”.



- Si eso no funciona, usaremos también las Address-List dinámicas





Verás que se generan dos: La “D” es de dinámica. Detecta la IP que usa youtube y la bloquea.

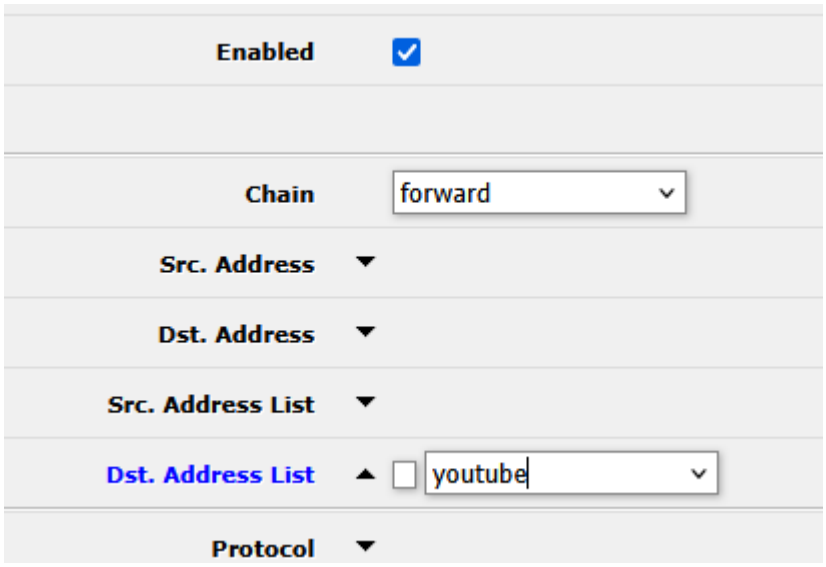
		Name	Address	Timeout	Creation Time
;;; youtube.com					
-	D	youtube	142.250.185.14		Jan/14/2026 11:39:51
- D		youtube	youtube.com		Jan/14/2026 11:39:49

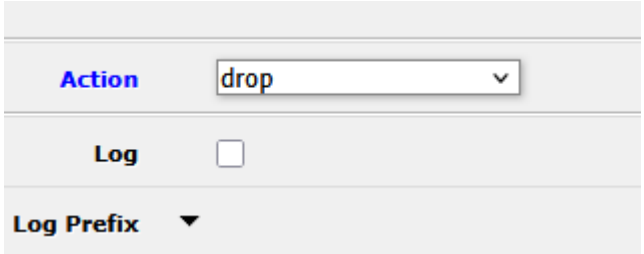
Ahora haremos lo mismo, pero con “googlevideo.com” y “ytimg.com”.

5 items

		Name	Address	Timeout	Creation Time
- D		youtube	ytimg.com		Jan/14/2026 11:41:46
;;; youtube.com					
-	D	youtube	142.251.140.238		Jan/14/2026 11:41:45
;;; googlevideo.com					
-	D	youtube	142.250.200.100		Jan/14/2026 11:41:25
- D		youtube	googlevideo.com		Jan/14/2026 11:41:25
- D		youtube	youtube.com		Jan/14/2026 11:39:49

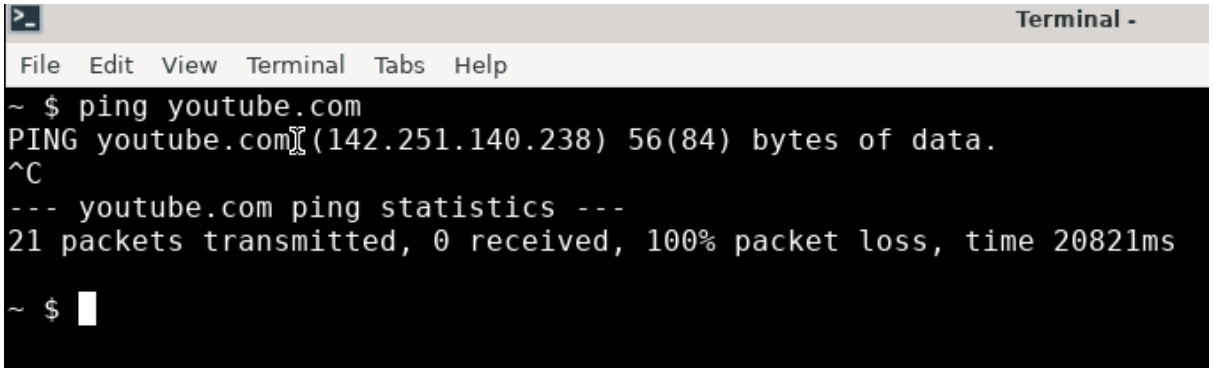
Para que tengan efecto, debemos crear una regla de filtrado: Firewall → Filter Rules.



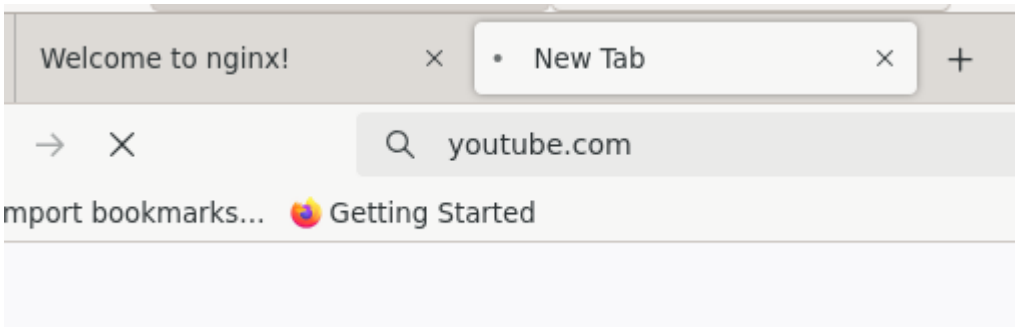


		#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In In
;;; Bloquear YouTube													
- D		0	drop	forward					6 (tcp)		443		
;;; Bloquear GoogleVideo													
- D		1	drop	forward					6 (tcp)		443		
;;; Bloquear YouTube completo													
- D		2	drop	forward				youtube					

Ahora el cliente no podrá acceder a YouTube.

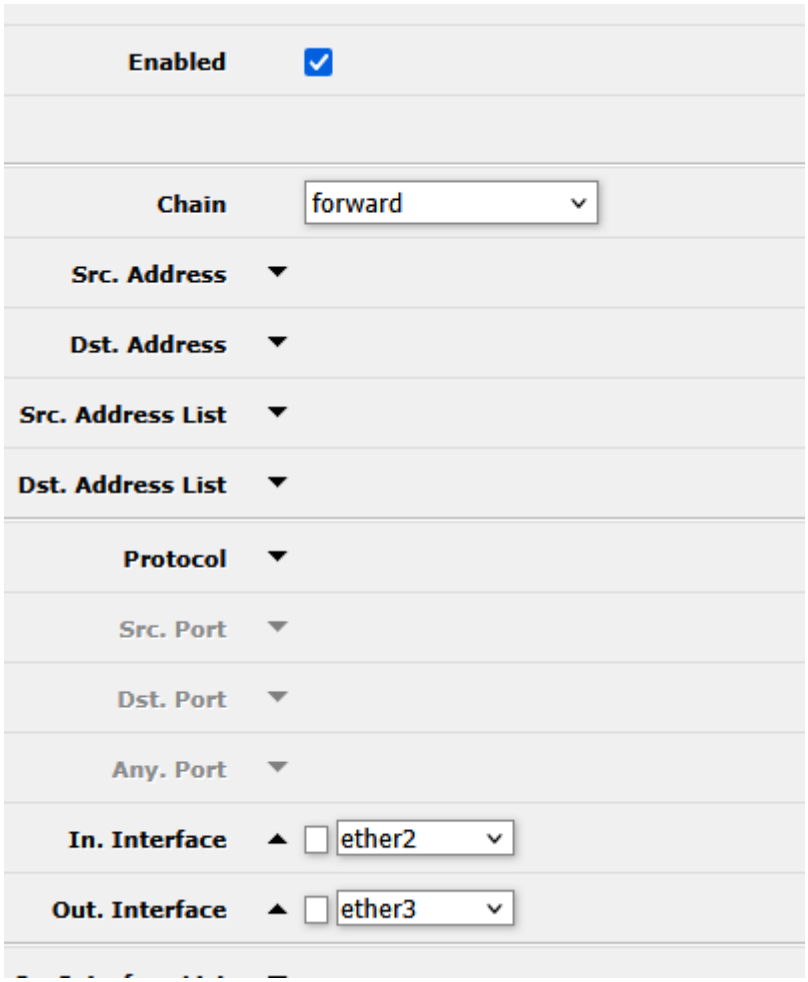


Youtube no podrá cargar.

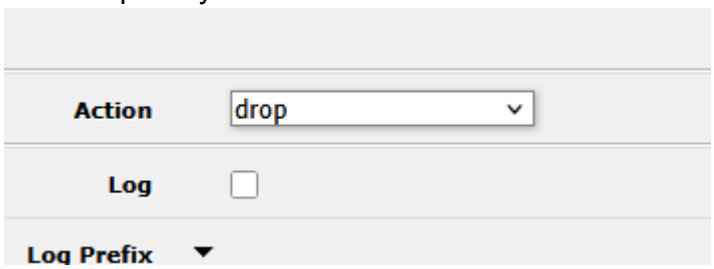


- Tarea 4: El "Silencio" del Cortafuegos (Problema de Política)
    - Intenta desde el cliente LAN hacer `ping` al servidor de la DMZ. ¿Qué ocurre?

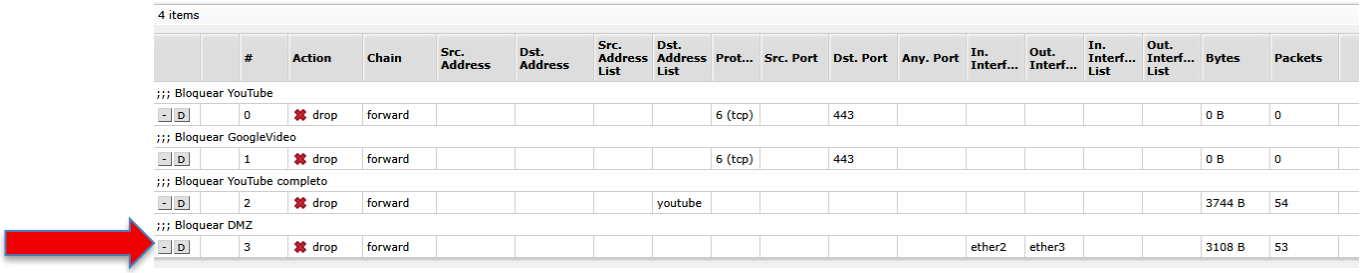
Con la configuración actual si se puede hacer. Vamos a modificarla para simular un caso en el que no podamos. Vamos a bloquear todo el tráfico de la LAN a la DMZ.



Todo lo que vaya desde la Ethernet2 a la Ethernet3 estará bloqueado.



Muy importante, las reglas más restrictivas deben poner al final del listado de reglas. En la interfaz web debes arrastrarla.



4 items

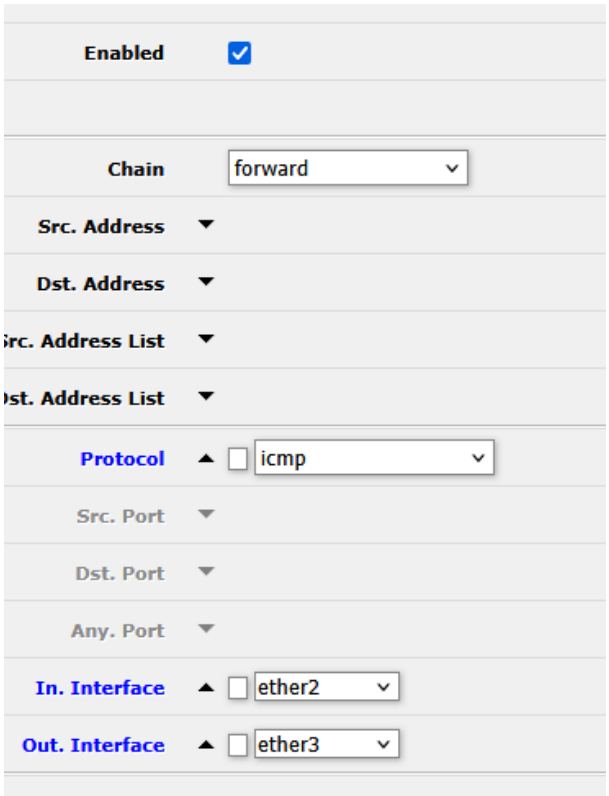
	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	In. Interf... List	Out. Interf... List	Bytes	Packets
;;; Bloquear YouTube																	
- D	0	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear GoogleVideo																	
- D	1	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear YouTube completo																	
- D	2	drop	forward				youtube									3744 B	54
;;; Bloquear DMZ																	
- D	3	drop	forward									ether2	ether3			3108 B	53

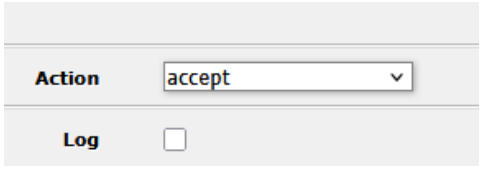
No puede hacer ping:

```
~ $ ping 172.16.0.50
PING 172.16.0.50 (172.16.0.50) 56(84) bytes of data.
^C
--- 172.16.0.50 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3160ms
```

- Habilita para que sea posible hacer ping al servidor DMZ desde LAN

Para solo hacer “ping”, debemos habilitar el protocolo “icmp”:





Debemos ponerlo como mínimo por encima del anterior, que era mucho más restrictivo.

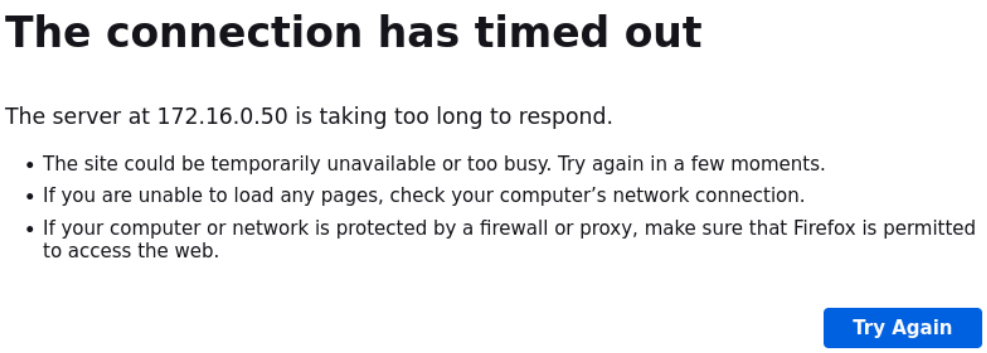
	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	In. Interf... List	Out. Interf... List	Bytes	Packets
;;; Bloquear YouTube																	
- D	0	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear GoogleVideo																	
- D	1	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear YouTube completo																	
- D	2	drop	forward				youtube									3744 B	54
;;; Permitir Ping a Servidor Nginx ICMP																	
- D	3	accept	forward					1 (icmp)				ether2	ether3			0 B	0
;;; Bloquear DMZ																	
- D	4	drop	forward									ether2	ether3			3108 B	53

Ahora puede hacer ping:

```
~ $ ping 172.16.0.50
PING 172.16.0.50 (172.16.0.50) 56(84) bytes of data.
64 bytes from 172.16.0.50: icmp_seq=1 ttl=63 time=7.08 ms
64 bytes from 172.16.0.50: icmp_seq=2 ttl=63 time=5.18 ms
64 bytes from 172.16.0.50: icmp_seq=3 ttl=63 time=5.08 ms
64 bytes from 172.16.0.50: icmp_seq=4 ttl=63 time=5.25 ms
^C
--- 172.16.0.50 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006m
```

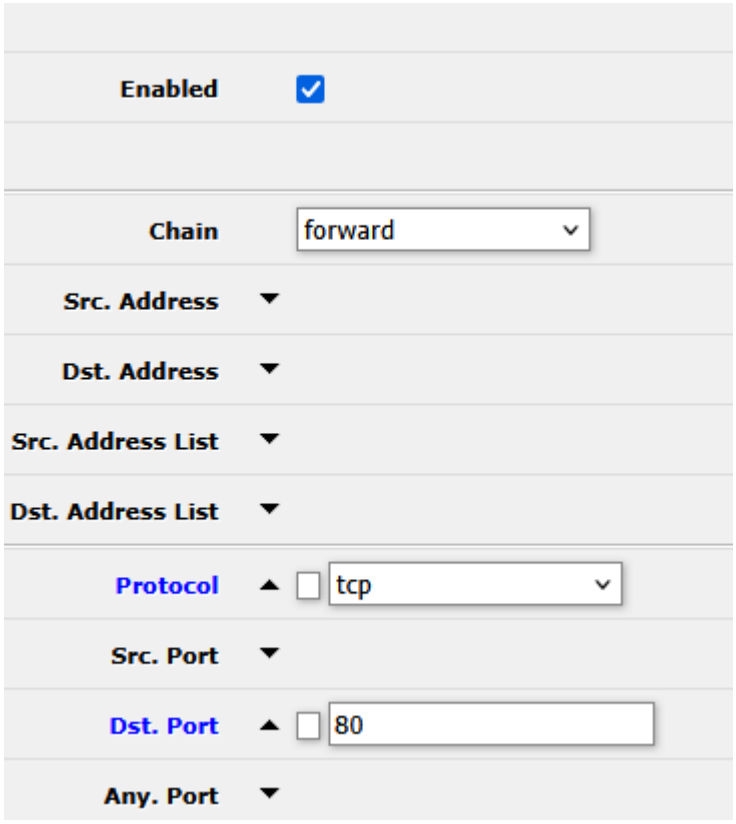
- Tarea 5: Acceso a servidor web DMZ
    - Intenta desde el cliente LAN ver la página web del servidor de la DMZ. ¿Qué ocurre?

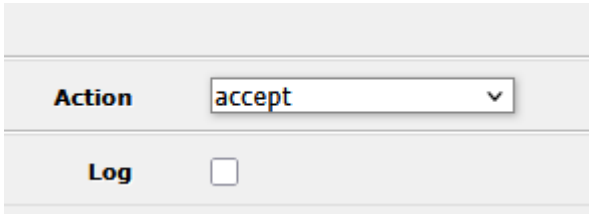
No será capaz de cargar la página del servidor:



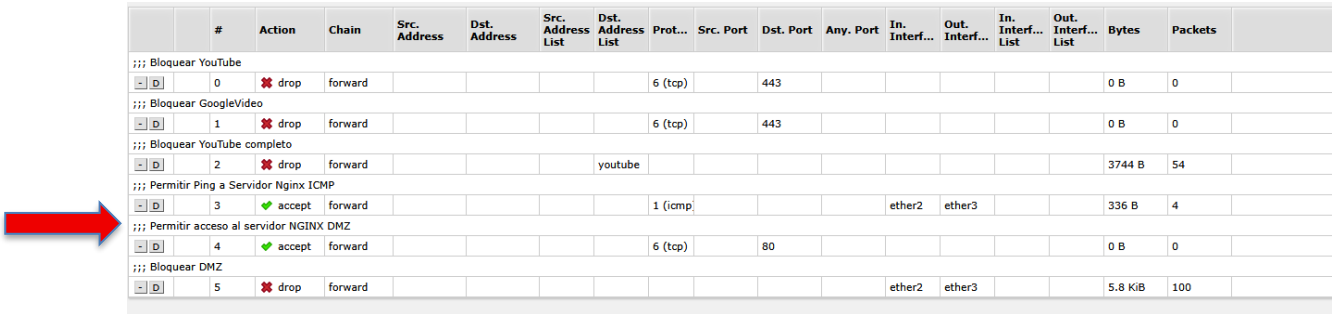
- Habilita para que sea posible ver la página web del servidor DMZ desde LAN

Abriremos el puerto 80 (Este servidor no usa SSL/TLS, así que no es necesario el 443).





E igual que con el otro, lo ponemos por encima del restrictivo.



	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	In. Interf... List	Out. Interf... List	Bytes	Packets
;;; Bloquear YouTube																	
- D	0	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear GoogleVideo																	
- D	1	drop	forward					6 (tcp)		443						0 B	0
;;; Bloquear YouTube completo																	
- D	2	drop	forward				youtube									3744 B	54
;;; Permitir Ping a Servidor Nginx ICMP																	
- D	3	accept	forward					1 (icmp				ether2	ether3			336 B	4
;;; Permitir acceso al servidor NGINX DMZ																	
- D	4	accept	forward					6 (tcp)		80						0 B	0
;;; Bloquear DMZ																	
- D	5	drop	forward									ether2	ether3			5.8 KiB	100

Y ahora carga perfectamente.