

# ACTIVIDAD 2 - FIREWALL MIKROTIK

Cristóbal Suárez Abad

SEGURIDAD Y ALTA DISPONIBILIDAD - 2º ASIR

## Diagrama en servidor GNS3 del Instituto: CSA\_Actividad\_2-Firewall Fortigate

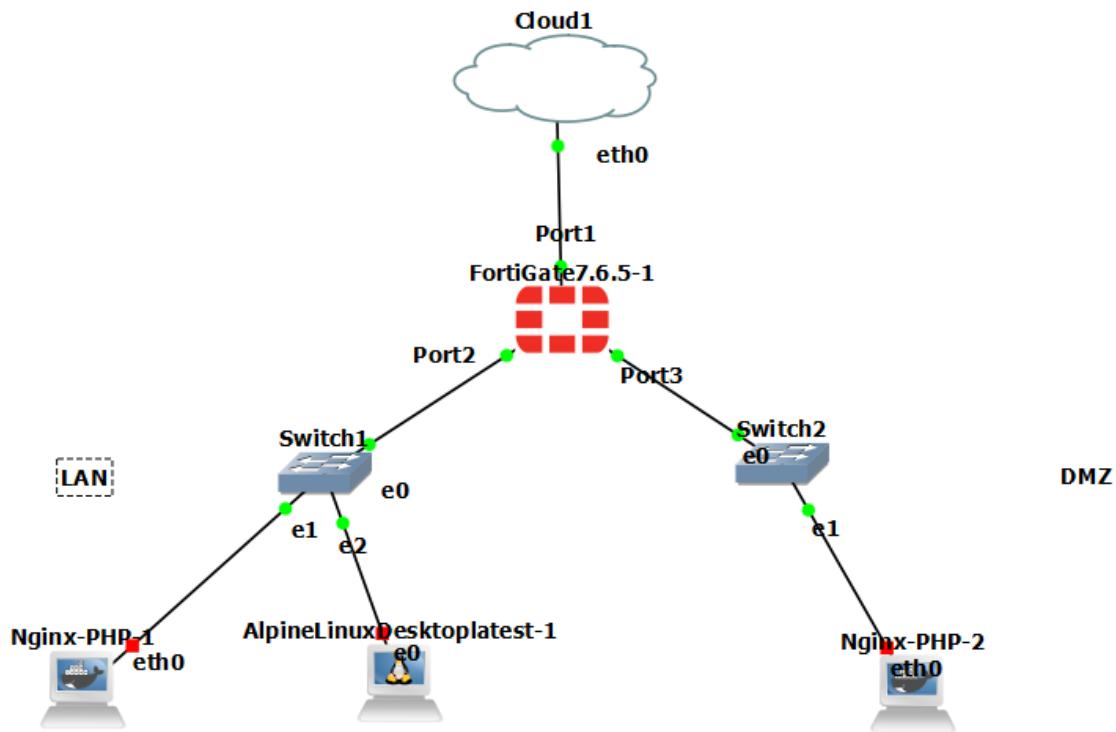
### Índice

<b>1. Escenario y Topología .....</b>	2
<b>2. Acceso a Mikrotik.....</b>	4
<b>3. Configuración de Red .....</b>	5
<b>4: Implementación de Cortafuegos.....</b>	7
• <b>Tarea 1: Salida a Internet: .....</b>	7
•     Tarea 2: Publicación de la DMZ (DNAT/VIP).....	11
• <b>¿Qué es un Virtual IP (VIP)? .....</b>	11
• <b>Tarea 3: Filtrado de Aplicaciones.....</b>	16
• <b>¿Por qué no basta con bloquear la IP?.....</b>	16
•     Tarea 4: El "Silencio" del Cortafuegos (Problema de Política) .....	22
•     Tarea 5: Acceso a servidor web DMZ.....	25

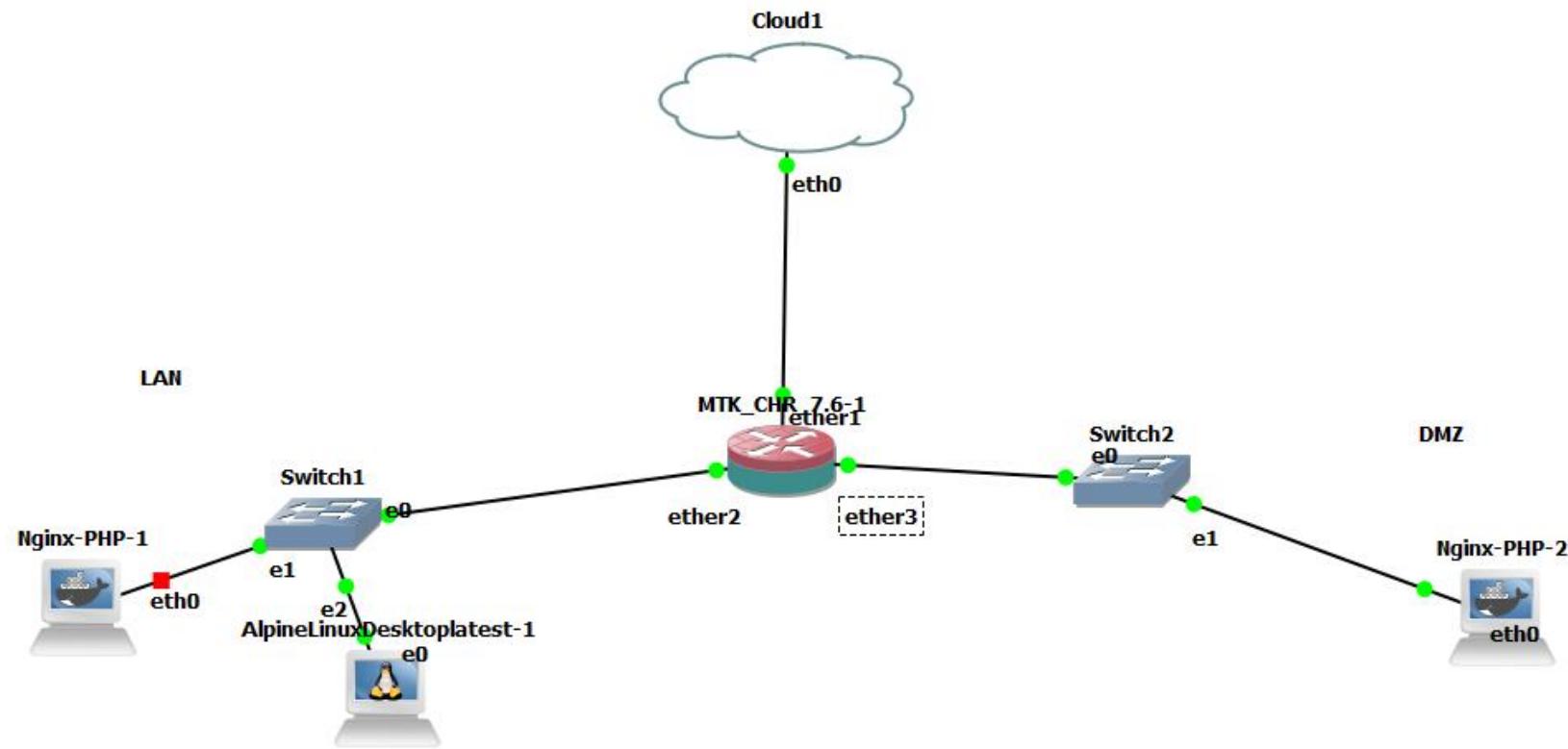
# 1. Escenario y Topología

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

```
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  192.168.2.1/24  192.168.2.0  ether4
3 D 10.255.1.82/21 10.255.0.0  ether1
[admin@MikroTik] >
```

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:

The screenshot shows the RouterOS v7.6 (stable) web interface. The URL in the browser is [http://10.255.1.82/webfig/#Quick\\_Set](http://10.255.1.82/webfig/#Quick_Set). The interface is titled "RouterOS v7.6 (stable)". The configuration mode is set to "Router". Under "Address Acquisition", "Automatic" is selected. The "IP Address" is set to 10.255.1.82, "Netmask" is 255.255.248.0 (/21), and "Gateway" is 10.255.0.1. The MAC address is listed as 0C:CD:F9:15:00:00. For the LAN port, the IP address is 192.168.2.1 and the netmask is 255.255.255.0 (/24). There is a checkbox for "Bridge All LAN Ports" which is unchecked.

### 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
```

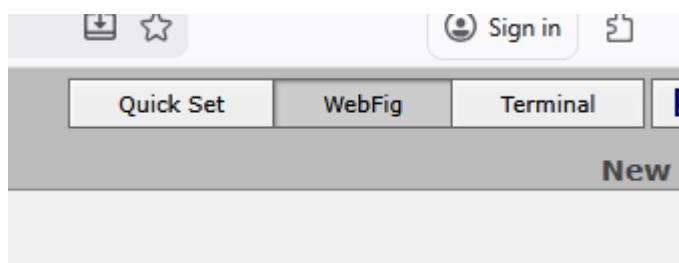
```
ip address/add address=172.16.0.1/24 interface=ether3
```

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.

Enabled	<input checked="" type="checkbox"/>
Address	192.168.10.1/24
Network	▼
Interface	ether2 ▼
Comment	

		Address	Network	Interface
-	D	10.255.1.82/21	10.255.0.0	ether1
-	D	172.16.0.1/24	172.16.0.0	ether3
-	D	192.168.10.1/24	192.168.10.0	ether2

## 4: Implementación de Cortafuegos

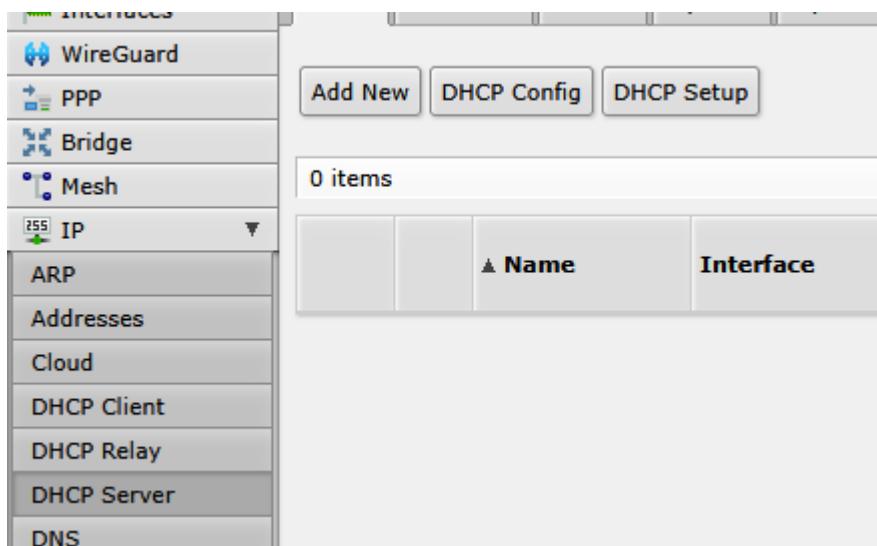
Configurar el Mikrotik desde cero (vía web en el cliente Alpine). Comprueba que funcionan los bloques y permisos, y documenta que el acceso es únicamente de la forma esperada.

- **Tarea 1: Salida a Internet:**

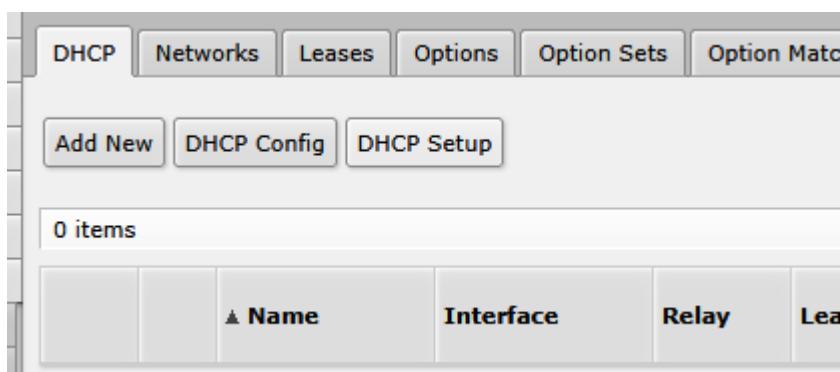
Configurar una política de LAN → WAN con NAT habilitado.

- *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.



Back    Next    Cancel

**DHCP Server Interface**    ether2 ▾

Add New    DHCP Config    DHCP Setup

2 items

	Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
- D	dhcp1	ether2		00:10:00	dhcp_pool4	no
- D	dhcp2	ether3		00:10:00	dhcp_pool5	no

Configuración del NAT.

Firewall → NAT

RouterOS v7.6 (stable)

Wireless    Interfaces    WireGuard    PPP    Bridge    Mesh

IP    ARP    Addresses    Cloud    DHCP Client    DHCP Relay    DHCP Server    DNS    Firewall    Hotspot

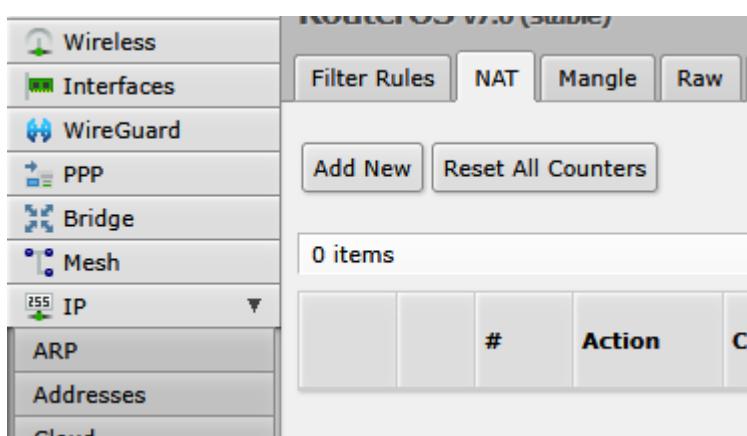
Filter Rules    NAT    Mangle    Raw    Service

Add New    Reset All Counters

1 item

	#	Action	Chain
- D	0	masquerade	srcnat

“Add new”



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

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Chain</b>	srcnat
<b>Src. Address</b>	▼
<b>Dst. Address</b>	▼
<b>Src. Address List</b>	▼
<b>Dst. Address List</b>	▼
<b>Protocol</b>	▼
<b>Src. Port</b>	▼
<b>Dst. Port</b>	▼
<b>Any. Port</b>	▼
<b>In. Interface</b>	▼
<b>Out. Interface</b>	ether1
<b>In. Interface List</b>	▼

En "Action" → "masquerade"

The screenshot shows a configuration window with the following fields:

- Action:** masquerade
- Log:**
- Log Prefix:** ▾
- To Ports:** ▾

Guardamos.

The screenshot shows a table with the following data:

	#	Action	Chain	Src. Address
-	D	0	masquerade	srcnat

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

```
rtr 10:07:45.414745.02070.595 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
c
```

## ● 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?

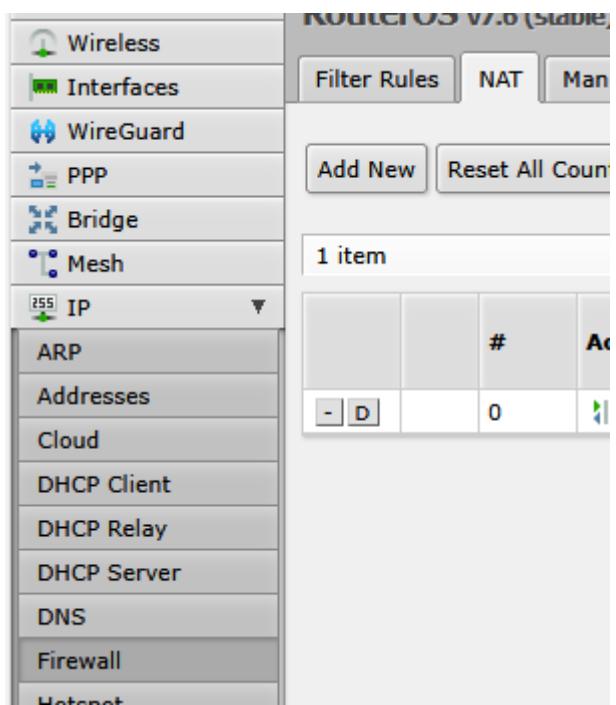
Es una técnica de red que permite que computadoras externas (desde Internet) se conecten a un dispositivo o servicio específico dentro de una red privada (LAN o DMZ) que estará mapeado en un puerto específico.

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.



<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Chain</b>	<input type="text" value="dstnat"/>
<b>Src. Address</b>	<input type="text"/>
<b>Dst. Address</b>	<input type="text"/>
<b>Src. Address List</b>	<input type="text"/>
<b>Dst. Address List</b>	<input type="text"/>
<b>Protocol</b>	<input type="text" value="6 (tcp)"/>
<b>Src. Port</b>	<input type="text"/>
<b>Dst. Port</b>	<input type="text" value="80"/>
<b>Any. Port</b>	<input type="text"/>
<b>In. Interface</b>	<input type="text" value="ether1"/>
<b>Out. Interface</b>	<input type="text"/>

“Chain” → dstnat

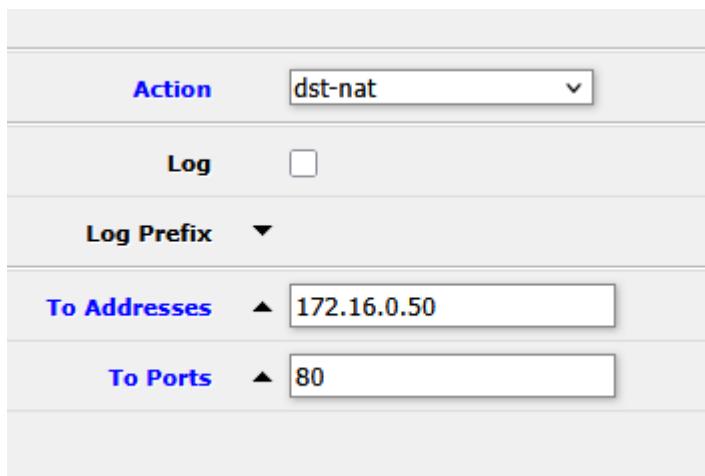
“Dst. Address” → La IP pública del router. En nuestro caso, al estar en laboratorio, no es realmente pública (tendríamos que usar la del Instituto, cosa que no podemos hacer); es la IP que conecta al router con el resto de internet.

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

“Dst. Port”: Usamos el puerto 80.

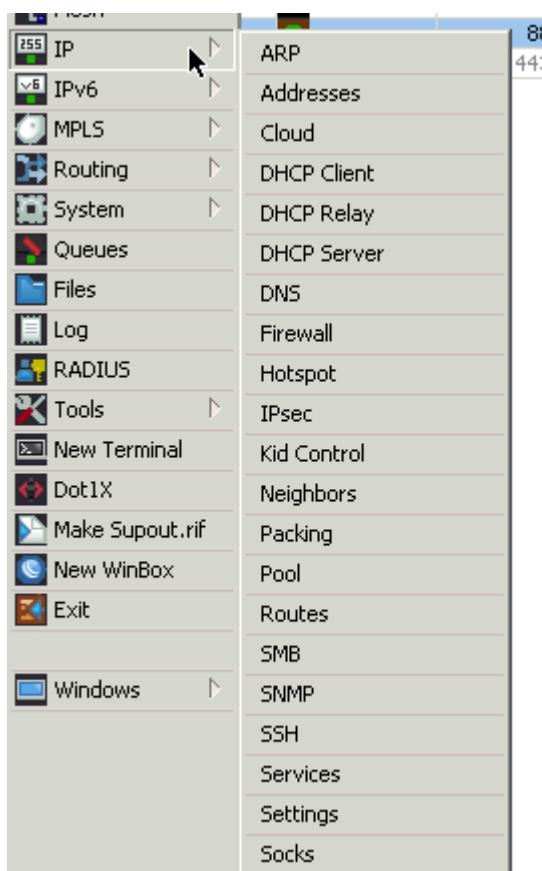
Luego nos vamos a “Action” y debemos seleccionar “dst-nat”.

Indicamos en “To Addresses” 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).

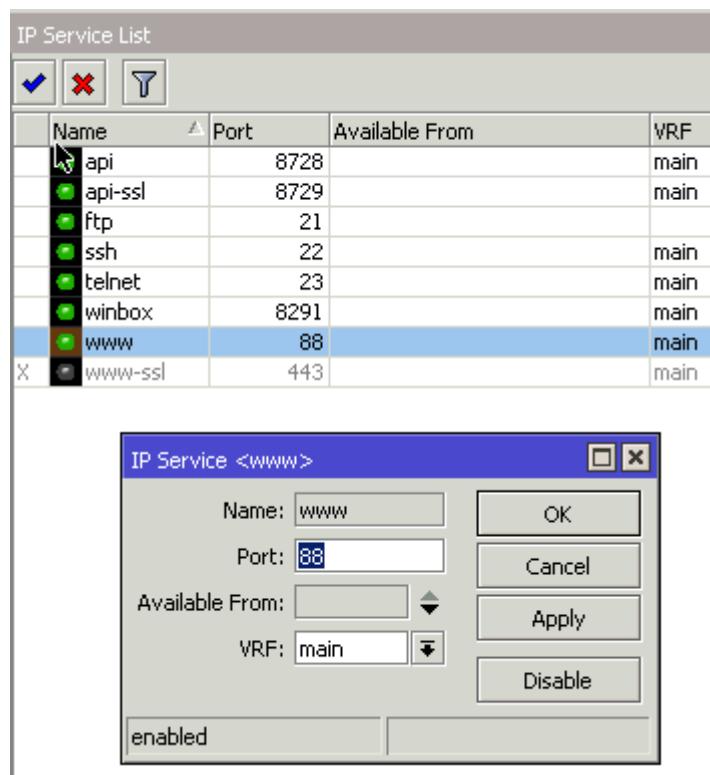


**ATENCIÓN: MUY IMPORTANTE:** Antes de darle a Apply o a OK y guardar la configuración, ten en cuenta que para acceder a la terminal de Mikrotik desde tu navegador, estas usando la IP “Pública” del router y usas el puerto 80. Si activas la configuración ahora te echará a fuera y no podrás seguir configurando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



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

## ● Tarea 3: Filtrado de Aplicaciones.

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

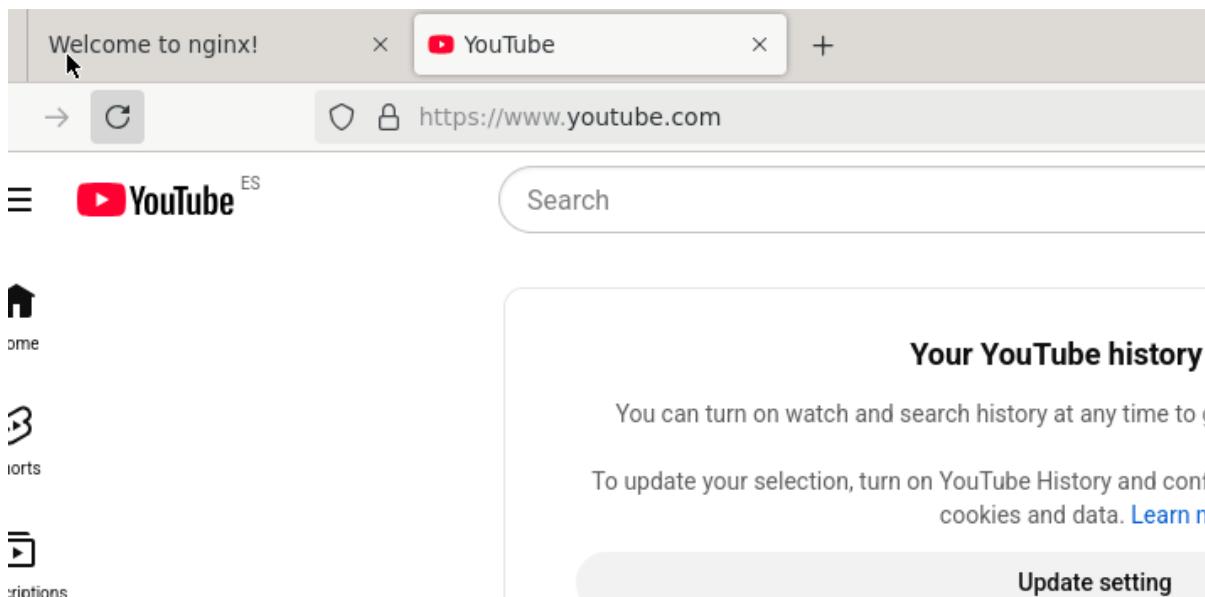
### ¿Por qué no basta con bloquear la IP?

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 mad4ls13-in-f14.1e100.net (142.250.200.110): icmp_seq=1 ttl=113 time=49.5 ms
64 bytes from mad4ls13-in-f14.1e100.net (142.250.200.110): icmp_seq=2 ttl=113 time=71.7 ms
64 bytes from mad4ls13-in-f14.1e100.net (142.250.200.110): icmp_seq=3 ttl=113 time=65.9 ms
64 bytes from mad4ls13-in-f14.1e100.net (142.250.200.110): icmp_seq=4 ttl=113 time=14.2 ms
^C
--- youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 30ms
rtt min/avg/max/mdev = 14.2/49.5/71.7/26.5 ms
```



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=ytiimg.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:

Enabled	<input checked="" type="checkbox"/>
Chain	forward
Src. Address	▼
Dst. Address	▼
Src. Address List	▼
Dst. Address List	▼
Protocol	▲ □ 6 (tcp) ▼
Src. Port	▼
Dst. Port	▲ □ 443 ▼
Any. Port	▼
IPsec Policy	▼
TLS Host	▲ □ *.youtube.com ▼
Ingress Priority	▼
Action	drop
Log	<input type="checkbox"/>
Log Prefix	▼

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

The screenshot shows a configuration window for an IPsec Policy. In the top left, there's a dropdown menu set to "IPsec Policy". Below it, a "TLS Host" field contains the value "\*.googlevideo.com". There are also dropdown menus for "Address Priority" and "IKEv1/IKEv2".

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

The screenshot shows a "Address Lists" configuration screen. On the left is a sidebar with various network-related options like Wireless, Interfaces, WireGuard, PPP, Bridge, Mesh, IP, ARP, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, and Firewall. The main area has tabs for Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7. A large "Add New" button is visible. Below it, a table header shows columns for Name, Address, Timeout, and Creation Time. The table body displays one item: "Name" is "youtube", "Address" is "youtube.com", and "Timeout" is set to "Never". At the bottom are buttons for OK, Cancel, and Apply.

	Name	Address	Timeout	Creation Time
	youtube	youtube.com	Never	Jan/14/2026 11:37:19

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

		Name	Address	Timeout	Creation Time
<b>;;; youtube.com</b>					
<input type="checkbox"/>	D	<input checked="" type="radio"/> youtube	142.250.185.14		Jan/14/2026 11:39:51
<input checked="" type="checkbox"/> D		<input checked="" type="radio"/> youtube	youtube.com		Jan/14/2026 11:39:49

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

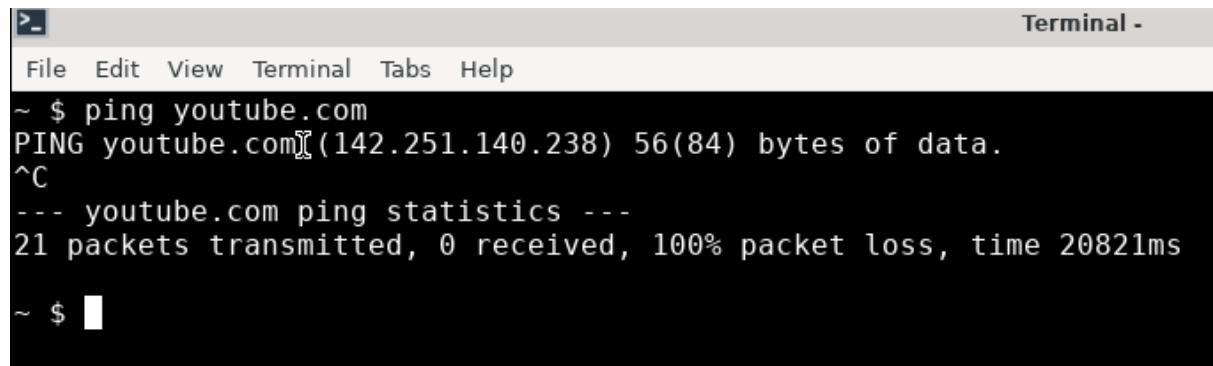
5 items					
		Name	Address	Timeout	Creation Time
<input type="checkbox"/> D		<input checked="" type="radio"/> youtube	ytmpg.com		Jan/14/2026 11:41:46
<b>;;; youtube.com</b>					
<input type="checkbox"/> D	D	<input checked="" type="radio"/> youtube	142.251.140.238		Jan/14/2026 11:41:45
<b>;;; googlevideo.com</b>					
<input type="checkbox"/> D	D	<input checked="" type="radio"/> youtube	142.250.200.100		Jan/14/2026 11:41:25
<input checked="" type="checkbox"/> D		<input checked="" type="radio"/> youtube	googlevideo.com		Jan/14/2026 11:41:25
<input checked="" type="checkbox"/> D		<input checked="" type="radio"/> youtube	youtube.com		Jan/14/2026 11:39:49

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

Enabled	<input checked="" type="checkbox"/>
Chain	forward
Src. Address	▼
Dst. Address	▼
Src. Address List	▼
Dst. Address List	▲ <input type="checkbox"/> youtube ▼
Protocol	▼
Action	drop
Log	<input type="checkbox"/>
Log Prefix	▼

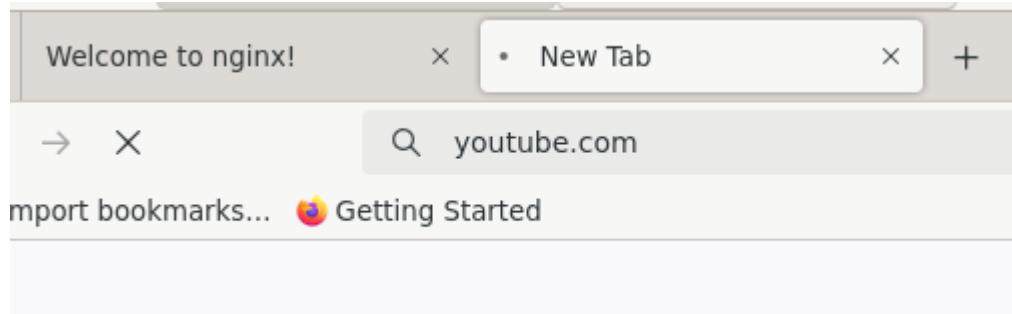
	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In In'
<b>::: Bloquear YouTube</b>												
-	D	0	drop	forward				6 (tcp)		443		
<b>::: Bloquear GoogleVideo</b>												
-	D	1	drop	forward				6 (tcp)		443		
<b>::: Bloquear YouTube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

Ahora el cliente no podrá acceder a YouTube.



```
File Edit View Terminal Tabs Help
~ $ ping youtube.com
PING youtube.com[142.251.140.238] 56(84) bytes of data.
^C
--- youtube.com ping statistics ---
21 packets transmitted, 0 received, 100% packet loss, time 20821ms
~ $
```

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.

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Chain</b>	forward
<b>Src. Address</b>	▼
<b>Dst. Address</b>	▼
<b>Src. Address List</b>	▼
<b>Dst. Address List</b>	▼
<b>Protocol</b>	▼
<b>Src. Port</b>	▼
<b>Dst. Port</b>	▼
<b>Any. Port</b>	▼
<b>In. Interface</b>	ether2
<b>Out. Interface</b>	ether3

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

<b>Action</b>	drop
<b>Log</b>	<input type="checkbox"/>
<b>Log Prefix</b>	▼

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



	#	Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Protocol	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Bytes	Packets
<b>;;: Bloquear YouTube</b>																	
- [D]	0	drop	forward					6 (tcp)		443						0 B	0
- [D]	1	drop	forward					6 (tcp)		443						0 B	0
- [D]	2	drop	forward				youtube									3744 B	54
- [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”:

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Chain</b>	forward
<b>Src. Address</b>	▼
<b>Dst. Address</b>	▼
<b>Src. Address List</b>	▼
<b>Dst. Address List</b>	▼
<b>Protocol</b>	icmp
<b>Src. Port</b>	▼
<b>Dst. Port</b>	▼
<b>Any. Port</b>	▼
<b>In. Interface</b>	ether2
<b>Out. Interface</b>	ether3
<b>Action</b>	accept
<b>Log</b>	<input type="checkbox"/>

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
<b>;;; Bloquear YouTube</b>																	
	0	✗ drop	forward					6 (tcp)		443						0 B	0
<b>;;; Bloquear GoogleVideo</b>																	
	1	✗ drop	forward					6 (tcp)		443						0 B	0
<b>;;; Bloquear YouTube completo</b>																	
	2	✗ drop	forward			youtube										3744 B	54
<b>;;; Permitir Ping a Servidor Nginx ICMP</b>																	
	3	✓ accept	forward					1 (icmp)				ether2	ether3			0 B	0
<b>;;; Bloquear DMZ</b>																	
	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 3006ms
```

## ● 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:



## The connection has timed out

The server at 172.16.0.50 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

[Try Again](#)

- 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).

**Enabled:**

**Chain:** **forward**

**Src. Address:** ▾

**Dst. Address:** ▾

**Src. Address List:** ▾

**Dst. Address List:** ▾

**Protocol:** ▲  **tcp** ▼

**Src. Port:** ▾

**Dst. Port:** ▲  **80**

**Any. Port:** ▾

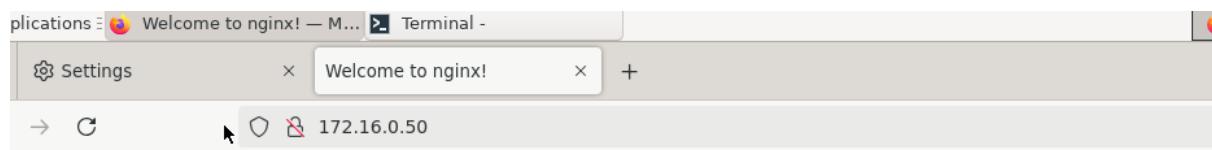
**Action:** **accept**

**Log:**

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	0	✗ drop	forward					6 (tcp)		443						0 B	0	
;;: Bloquear GoogleVideo	1	✗ drop	forward					6 (tcp)		443						0 B	0	
;;: Bloquear YouTube completo	2	✗ drop	forward				youtube									3744 B	54	
;;: Permitir Ping a Servidor Nginx ICMP	3	✓ accept	forward					1 (icmp)				ether2	ether3			336 B	4	
;;: Permitir acceso al servidor NGINX DMZ	4	✓ accept	forward					6 (tcp)		80						0 B	0	
;;: Bloquear DMZ	5	✗ drop	forward									ether2	ether3			5.8 KiB	100	

Y ahora carga perfectamente.



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*