

MUM – Mexico 2018

Filtrado por DNS

Por: Ing. José Miguel Cabrera
Ecatel SRL



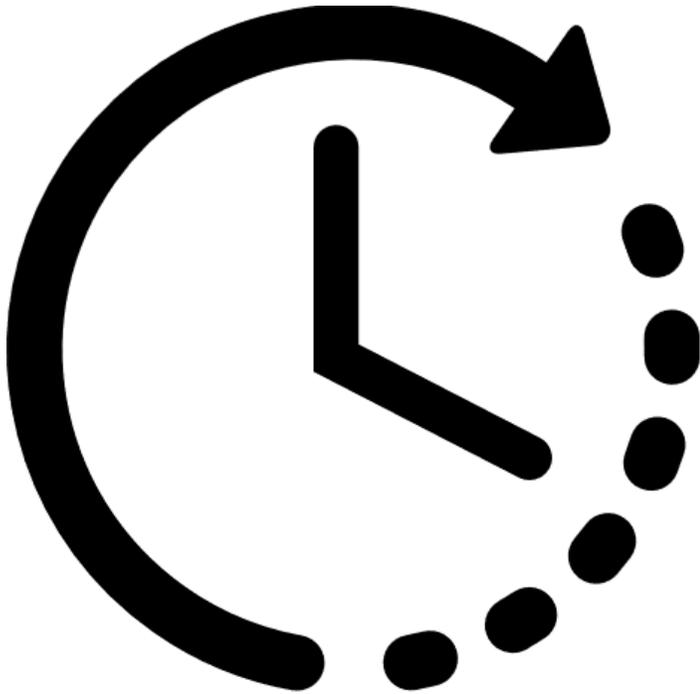
Resumen

Cada vez que ingresamos el nombre de una página web en la barra de direcciones (<https://ecatel.com.bo/>), la PC consulta a un servidor DNS para averiguar la dirección IP (194.180.140.130) de la página.

Se puede utilizar el Servidor DNS para dirigir ese tráfico hacia otra IP con la finalidad de impedir esta conexión. Por ejemplo: evitar la infección de algún malware o pornografía



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de DNS
- Como funciona un filtro por DNS
- Demostración



Acerca de la empresa

Es una empresa que se dedica a la **implementación de proyectos** integrando principalmente equipos de la marca Mikrotik, si es necesario combinados con otras marcas.

Brindamos **capacitaciones de MikroTik**.

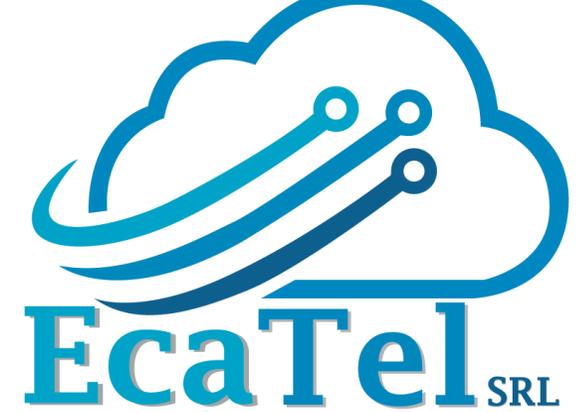
Contáctenos

info@ecatel.com.bo

+591 776 25848



facebook.com/EcatelSRL



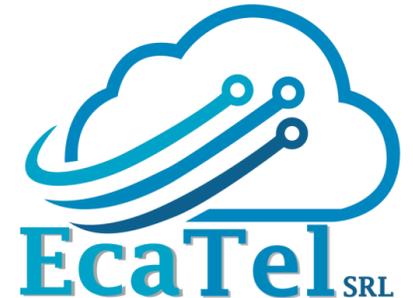
Acerca del disertante

- **Nombre:** Jose Miguel Cabrera Dalence
- **Nacionalidad:** Boliviano 
- **Profesión:** Ing. en Redes y Telecomunicaciones (UTEPSA)
- **Posgrado:** Especialista en Educación Superior Tecnológica (UAGRM)



Experiencia Laboral:

- Gerente de Proyectos en Ecatel SRL (2015 a la fecha)
- Instructor Mikrotik (2015 a la fecha)
- Jefe Nacional de Telecomunicaciones Banco Fassil (2010-2015)
- Docente Universitario en Utepsa y UAGRM (2011-2016).



Acerca del disertante

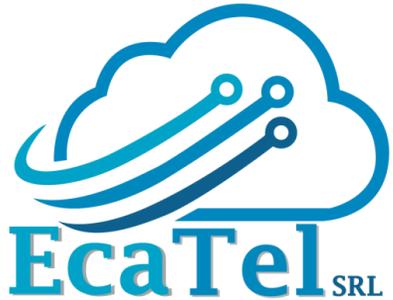
Certificaciones:



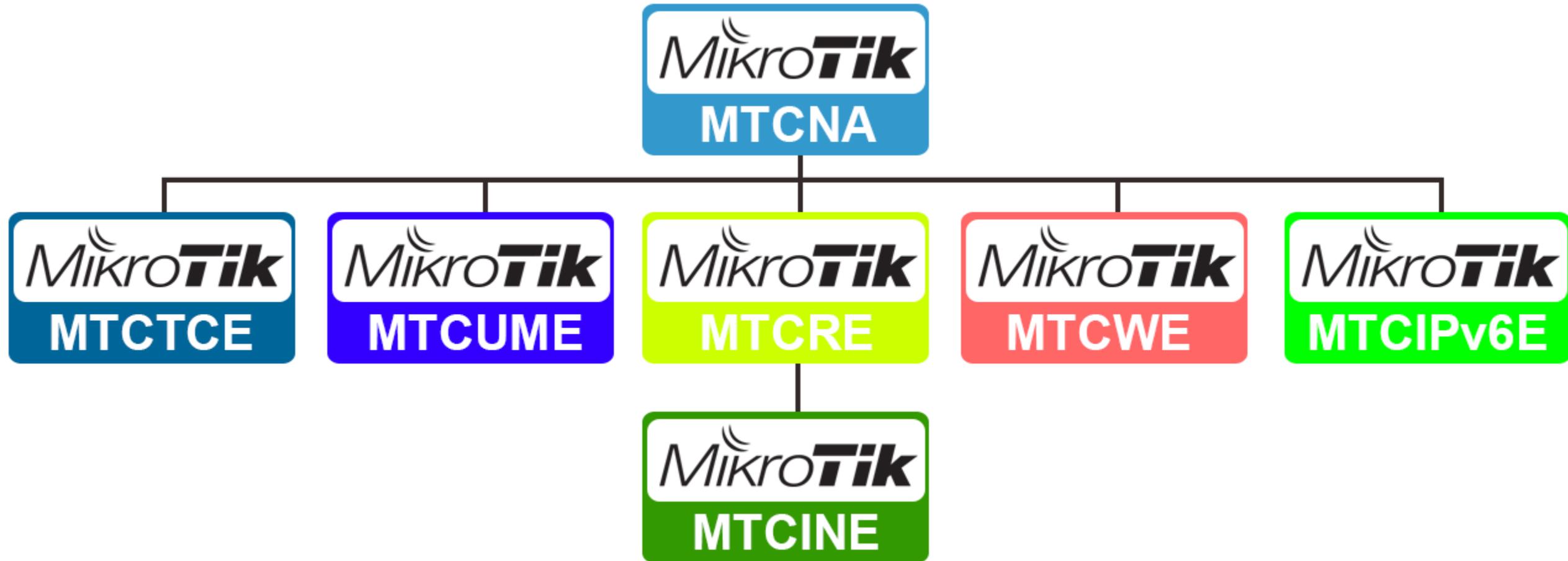
- **Mikrotik:** MTCNA, MTCWE, MTCRE, MTCINE, MTCUME, MTCTE, MTCIPv6E, Trainer
- **Cisco:** CCNP Security, CCNA R&S, CCNA Security

Conferencias y Capacitaciones:

- **Conferencista:** Argentina, Bolivia, México, Paraguay y Uruguay.
- **Se capacitó en:** Bolivia, Perú, Ecuador y Estados Unidos
- **Entrenador MikroTik:** Bolivia, Chile, México, Paraguay, Perú y Uruguay



Programa de Certificaciones



Ciudad de Mexico, Mexico

PROXIMO CURSO: ABRIL 2018

MTCNA

Miércoles 18, Jueves 19 y Viernes 20 de Abril

Desde las 09:00 am - 06:00pm

Sede: Empresa Syscom Norte



MTCUME

Sábado 21 y Domingo 22 de Abril

Desde las 09:00 am - 06:00pm

Sede: Empresa Syscom Norte



Ciudad de Mexico, Mexico

PROXIMO CURSO: JUNIO 2018

MTCNA

Viernes 15, Sábado 16 y Domingo 17 de Junio

Desde las 09:00 am - 06:00pm

Sede: Empresa Syscom Norte



MTCRE

Lunes 18 y Martes 19 de Junio

Desde las 09:00 am - 06:00pm

Sede: Empresa Syscom Norte



Mazatlan, Mexico

PROXIMO CURSO: JUNIO 2018

MTCNA

Viernes 22, Sábado 23 y Domingo 24 de Junio

Desde las 09:00 am - 06:00pm



MTCRE

Lunes 25 y Martes 26 de Junio

Desde las 09:00 am - 06:00pm





Objetivos Del Curso **MTCNA**

- Proporcionar una visión general del software RouterOS y los productos RouterBoard
- Obtener destrezas prácticas en configuración, mantenimiento y resolución de problemas básicos para dispositivos MikroTik RouterOS



Contenido del **MTCNA**

- Capitulo 1: Introducción
- Capitulo 2:DHCP
- Capitulo 3:Bridging
- Capitulo 4:Routing
- Capitulo 5:Wireless
- Capitulo 6:Firewall
- Capitulo 7:QoS
- Capitulo 8:Tuneles VPN
- Capitulo 9:Herramientas





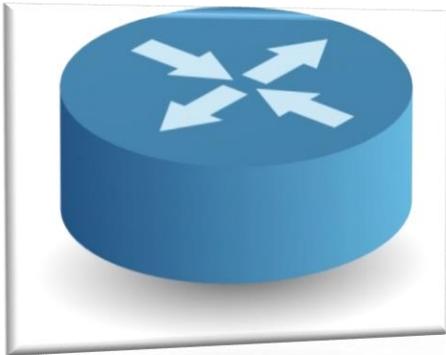
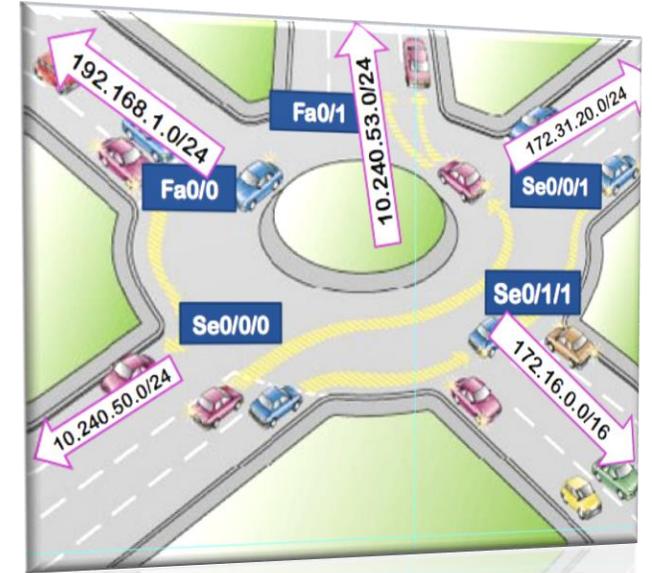
Objetivos Del Curso **MTCRE**

Al final de esta sesión de entrenamiento, el estudiante será capaz de planificar e implementar enrutamiento en dispositivos RouterOS Mikrotik. Tanto de manera estática o dinámica



Contenido del curso **MTCRE**

- **Capitulo 0:** Repaso MTCNA
- **Capitulo 1:** Enrutamiento Estatico
- **Capitulo 2:** Enrutamiento Punto a Punto



- **Capitulo 3:** Enrutamiento InterVLAN y VPN
- **Capitulo 4:** Enrutamiento Dinamico
(OSPF)





MERCADOWISP MEXICO

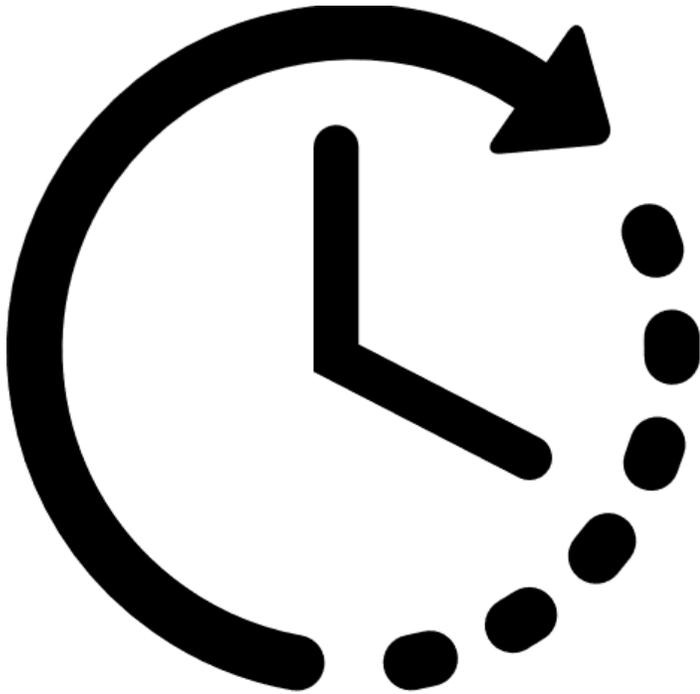
GRATIS

**Participa de una rifa de becas
para cursos**

<https://ecatel.com.mx/formmx>



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- **Conceptos de DNS**
 - Como funciona un filtro por DNS
 - Demostración



DNS

DNS (Domain Name System - Sistema de nombres de dominio) es un protocolo que convierte nombres de dominio a direcciones IP.

Ejemplo:

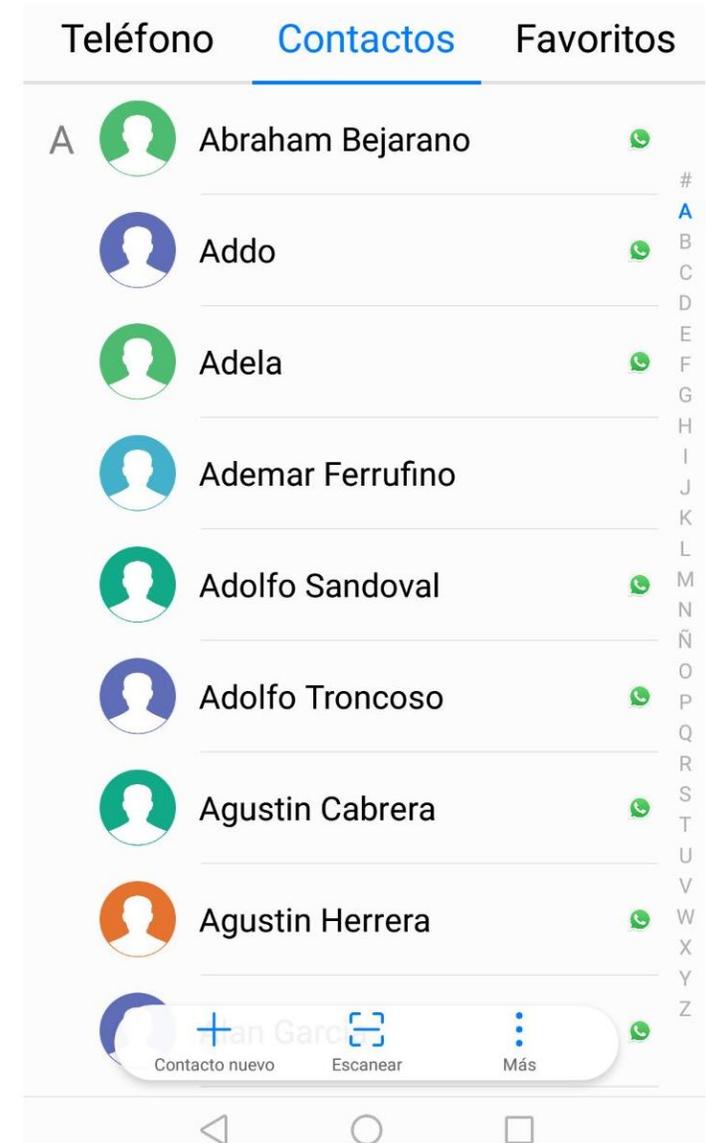
www.mikrotik.com = 159.148.147.196





DNS

Es muy parecido a una Guía Telefónica o los contactos de tu celular, tu buscas el nombre de la persona y obtienes el número de teléfono.



Servidor DNS

Sin un servidor DNS no se puede navegar en Internet. Es por eso que nuestro ISP nos proporciona un servidor DNS (una IP).

Como es un protocolo vital para la navegación, es normal que te brinden un Servidor DNS alternativo.



Servidor DNS

Es común, que el ISP no permita consultas DNS (bloqueado por firewall) de cualquier IP. Solamente desde sus clientes.



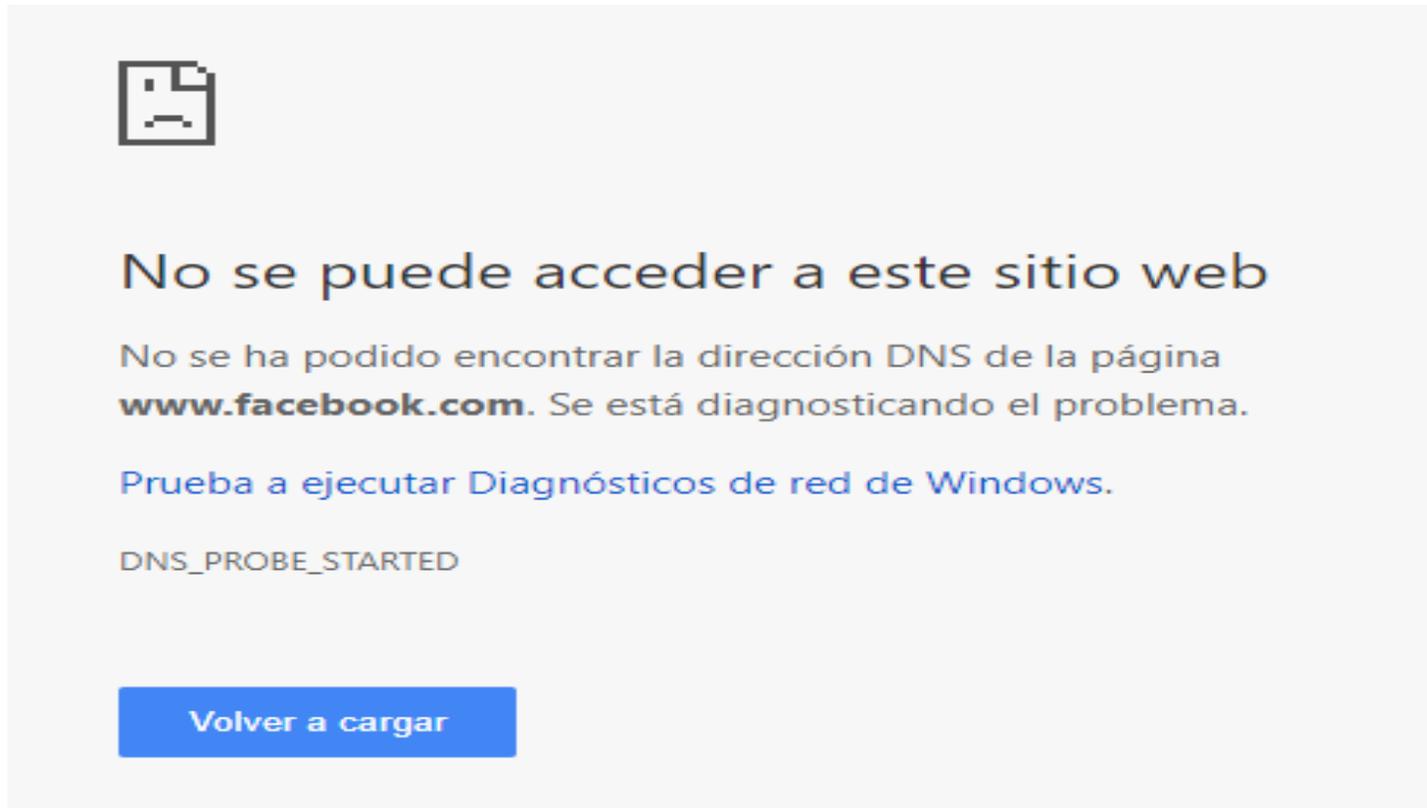
¿Qué pasa cuando balanceo 2 conexiones de Internet de distintos proveedores?



Problema con el DNS

Entonces algunas consultas DNS serán rechazadas y nuestro navegador

mostrará



Servidores DNS

- En ese momento quieres utilizar un servidor externo (como el de Google 8.8.8.8)
- Pero la latencia puede ser un problema
- Mikrotik en el RouterOS puede actuar como un Cache de DNS, es decir, el puede recibir las consultas, reenviarlas y almacenar las respuestas



Habilitar DNS-Server

The screenshot displays the Mikrotik WinBox interface for configuring a DNS server. The left sidebar shows the 'IP' menu item highlighted with a red box and the number 1. The middle menu shows the 'DNS' option highlighted with a red box and the number 2. The right configuration panel, titled 'DNS Settings', contains several fields and buttons. The 'Servers' field is highlighted with a red box and the number 3, showing the values '8.8.8.8' and '8.8.4.4'. The 'Allow Remote Requests' checkbox is checked and highlighted with a red box and the number 4. The 'Cache Max TTL' field is highlighted with a red box and the number 5, showing the value '01:00:00'. The 'OK' button is highlighted with a red box and the number 6. Other fields include 'Dynamic Servers', 'Max UDP Packet Size' (4096), 'Query Server Timeout' (2.000 s), 'Query Total Timeout' (10.000 s), 'Cache Size' (2048 KB), and 'Cache Used' (10).





ADVERTENCIA

- Proteja su router, **NO** permita las consultas desde redes externas (Internet). Con una regla de Firewall Filter haga DROP al tráfico udp/53 que provenga desde su interfaz hacia Internet. Si tiene IP Publica Fija y **NO hace esto**, tendrá consumo del ancho de banda y CPU excesivo.





Reglas de Firewall

Creamos una lista de interfaces, para identificar la LAN

Suponemos que la ether2 es parte de la LAN (podiera ser bridge1)

```
/interface list  
add name=RedLocal  
/interface list member  
add interface=ether2 list=RedLocal
```



Reglas de Firewall



Descartamos consultas DNS externas a la **RedLocal**

```
/ip firewall raw
add action=drop chain=prerouting dst-port=53 \
in-interface-list=!RedLocal protocol=udp

add action=drop chain=prerouting dst-port=53 \
in-interface-list=!RedLocal protocol=tcp
```



DNS FLOOD

Amplificación

Ataque de amplificación de DNS, es un ataque DDoS asimétrico. Supongamos que la víctima (otro DNS Server) tiene la IP 1.2.3.4 el atacante envía una pequeña consulta DNS con una IP de origen falsa (la de su víctima), haciendo que las respuestas vayan hacia la víctima. Con estos ataques, el objetivo del atacante es saturar la red agotando continuamente la capacidad de ancho de banda.



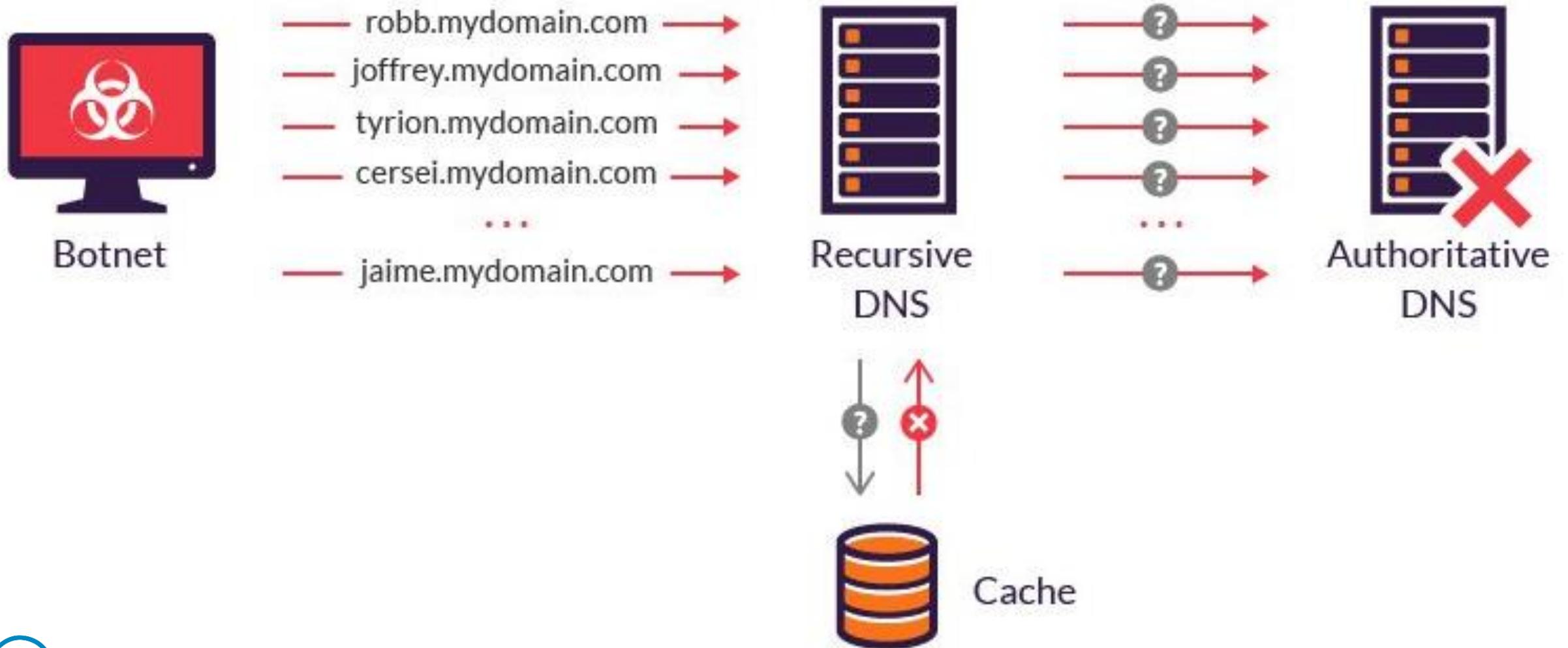
DNS FLOOD

Inundación

Ataque de inundación de DNS, son ataques DDoS simétricos. Estos ataques intentan agotar los activos del propio servidor DNS (por ejemplo: ancho de banda, memoria o CPU) con una avalancha de solicitudes UDP, generadas por scripts que se ejecutan en varias máquinas botnet comprometidas.



ESQUEMA - DNS FLOOD



Aplicar DNS

Una vez tenemos listo nuestro DNS en el MikroTik tenemos un par de alternativas para hacer que los usuarios lo utilicen.

- En el DHCP Server colocar la IP del router como el DNS.
- En Firewall/NAT hacer una regla en la cadena DSTNAT para aplicarlo de manera transparente.
- Aplicar las 2 anteriores al mismo tiempo.



DNS por DHCP Server

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'IP' menu item is highlighted with a red box and a red '1'. In the main menu, 'DHCP Server' is highlighted with a red box and a red '2'. The 'DHCP Server' configuration window is open, with the 'Networks' tab selected and highlighted with a red box and a red '3'. A table of DHCP networks is displayed, with the 'DNS Servers' column highlighted by a red box and a red '4'. The table contains the following data:

Address	Gateway	DNS Servers
172.18.0.0/24	172.18.0.1	172.18.0.1
172.30.16.0/24	172.30.16.1	172.30.16.1
192.168.1.0/24	192.168.1.1	192.168.1.1
192.168.2.0/24	192.168.2.1	192.168.2.1
192.168.8.0/24	192.168.8.1	192.168.8.1
192.168.9.0/24	192.168.9.1	192.168.9.1
192.168.12.0/24	192.168.12.1	192.168.12.1
192.168.36.0/24	192.168.36.1	192.168.36.1
192.168.79.0/24	192.168.79.254	192.168.79.254

At the bottom of the window, it says '9 items (1 selected)'.

DNS Transparente

Debes aplicar el siguiente comando:

```
/ip firewall nat  
  add chain=dstnat protocol=udp dst-port=53 \  
  in-interface-list=RedLocal \  
  place-before=0 \  
  action=redirect
```



¿Por qué ambos?



Sería muy sencillo para el usuario final cambiar sus Servidores de DNS (principal y alternativo) dejando nuestra técnica de cache sin uso (y posterior filtrado)



Eliminar Cache DNS

The image shows two windows from a network configuration utility. The left window is titled "DNS Settings" and contains various configuration options. The "Cache" button is highlighted with a red box and labeled with a large red "1". The right window is titled "DNS Cache" and displays a table of cached DNS records. The "Flush Cache" button is highlighted with a red box and labeled with a large red "2".

DNS Settings

Servers: 200.58.160.25
200.58.161.25

Dynamic Servers:

Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Cache Size: 2048 KB

Cache Max TTL: 7d 00:00:00

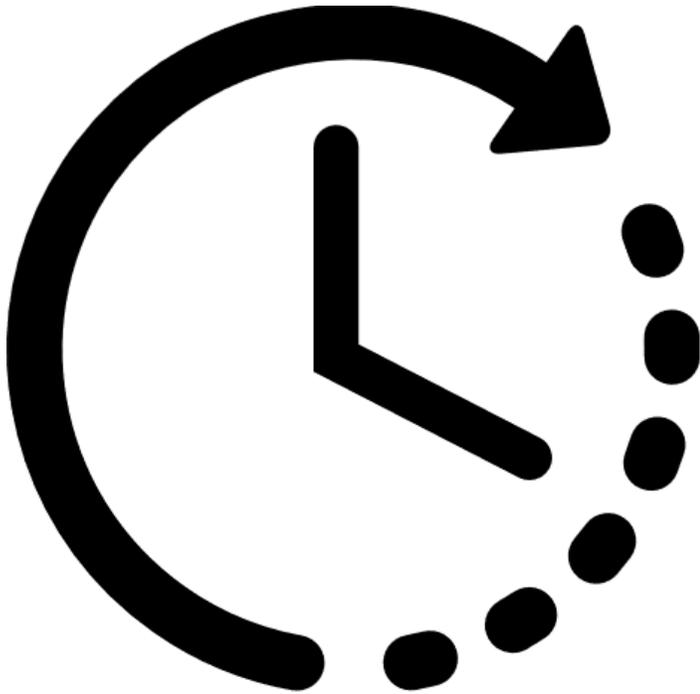
Buttons: OK, Cancel, Apply, Static, **Cache**

DNS Cache

Name	Type	Data	TTL
0-edge-chat.facebook.com	CNAME	star.c10r.facebook.com	00:18:21
0ff7bb0229e6.bitsngo.net	CNAME	bngcloud.vo.llnwd.net	19:45:53
1-courier.push.apple.com	CNAME	1.courier-push-apple.co...	03:40:10
1-edge-chat.facebook.com	CNAME	star.c10r.facebook.com	00:19:44
1-ps.googleusercontent.c...	CNAME	googlehosted.l.googleus...	20:04:55
1.bp.blogspot.com	CNAME	photos-ugc.l.googleuser...	4d 02:10:28
1.cdn1.image.extremetub...	CNAME	cdn1.image.extremetube...	03:09:40
1a4s4dv.m.ns1p.net	CNAME	tata.atanar.net	00:12:53
1aca.vd.aclst.com	A	37.187.142.102	1d 17:28:33
1c38.vd.aclst.com	A	5.196.82.170	3d 18:00:55
1d245-lb.wpc.xicdn.net	CNAME	lb.apr-1d245.edgecastd...	00:12:47
1f0e.vd.aclst.com	A	37.187.171.54	1d 16:01:38
1ff1.vd.aclst.com	A	37.187.170.85	2d 19:38:50
1s2qvh91x.site.aplus.net	A	64.29.151.221	00:32:18



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de DNS
- **Como funciona un filtro por DNS**
- Demostración



Filtrado de contenido



Muchas son las veces que nos piden bloquear el acceso a páginas web como: Facebook, Instagram, web de apuestas deportivas, páginas para adultos... Existen múltiples soluciones para hacerlo



Malware

En la actualidad las fuentes más populares de infección de malware son:

- 1) Navegación en Internet
- 2) Correo Electrónico
- 3) Vulnerabilidades del Software
- 4) Medios extraíbles

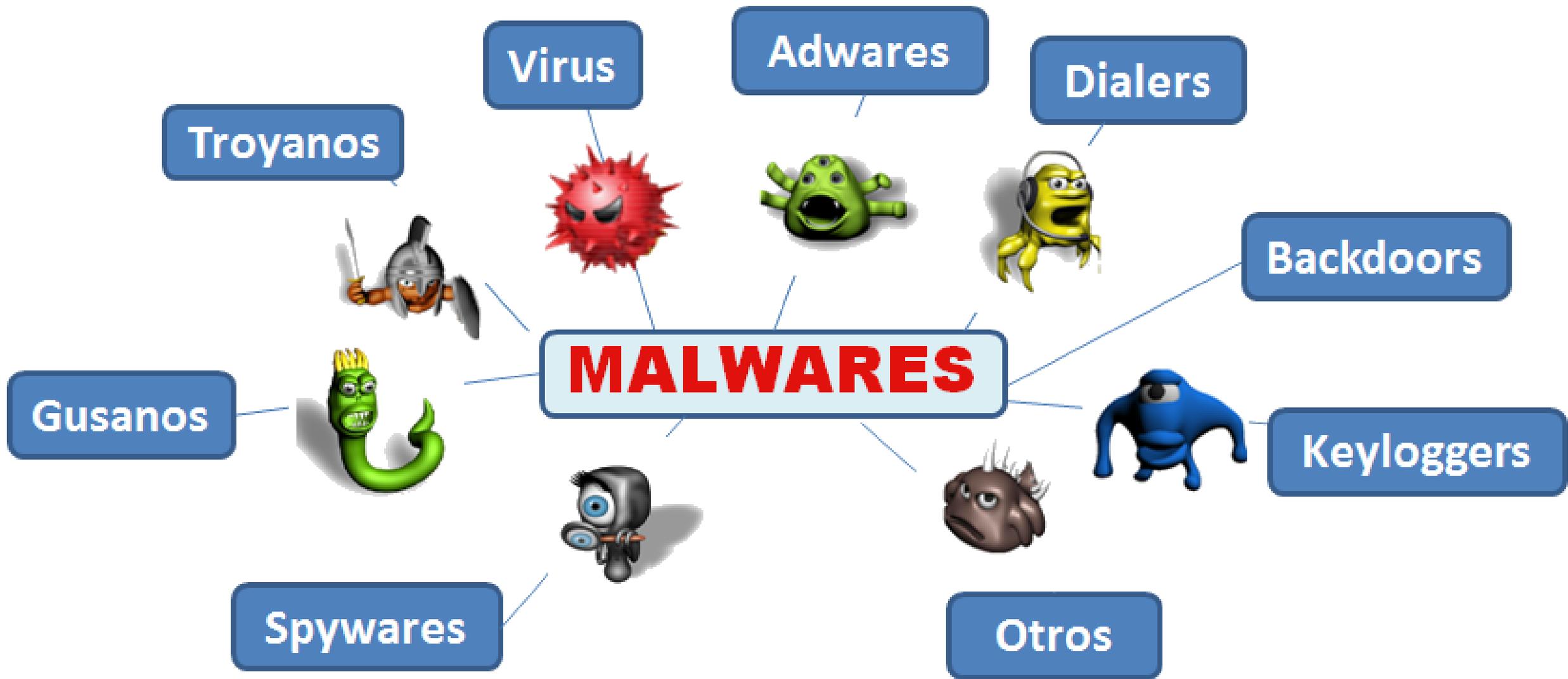


Malware

Como administradores de la red, podemos evitar 2 fuentes de infección:

- 1) Navegación en Internet
- 2) Correo Electrónico
- 3) Vulnerabilidades del Software
- 4) Medios extraíbles





¿Qué es Malware?

Del inglés **malicious software**, programa malicioso, es el término para referirse a:

- Backdoor
- Virus
- Troyano
- Gusanos
- Spyware
- Adware
- Hijacking
- Ransomware
- Botnets
- Keyloggers



FlashStart INTERNET PROTECTION

- » **Fundada en el 2001 enfocada al Acceso a Internet Access**
- » Aproximadamente atiende 1 000 millones de consultas DNS por día
- » Más de 50 categorías y subcategorías en el Blacklist
- » **Detiene más de 250 000 sitios que contienen Malware**



Solo vende mediante resellers



**100% de ventas indirectas
Nunca venden directamente**



Aman los canales de distribución



FlashStart INTERNET PROTECTION

FlashStart es una tecnología de filtrado de Internet por DNS. Mitiga malware, es una solución en la nube y puedes ser utilizada por grandes, medianas o pequeñas empresas, instituciones educativas, Gobierno y cualquier otra persona. FlashStart **no requiere hardware o software adicional** y se integra fácilmente con dispositivos **MikroTik**. En tan sólo 5 minutos, FlashStart puede ser conectado, ofrecer filtrado y monitoreo sin complicaciones.

<http://www.flashstart.com/>



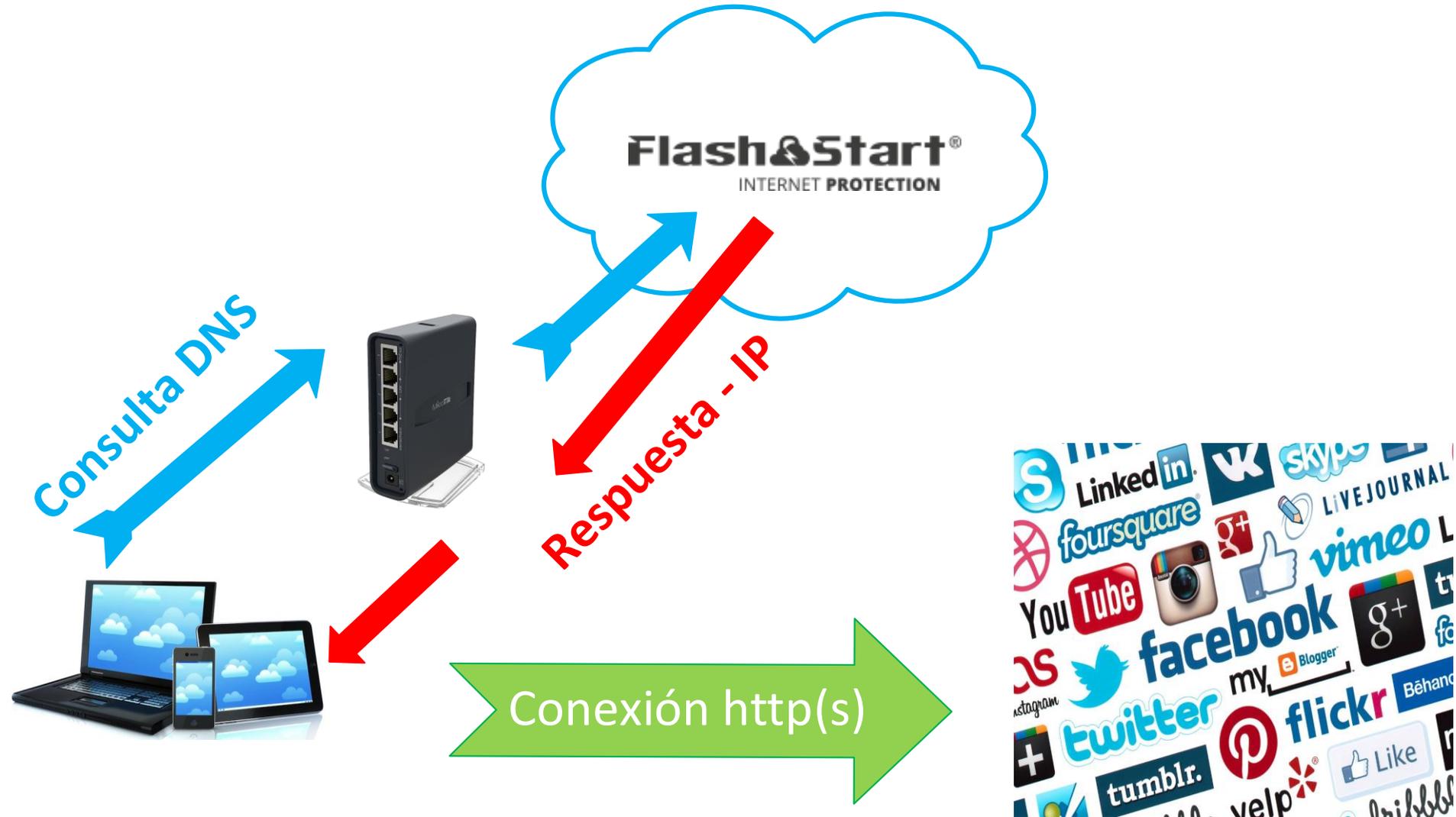
¿Cómo funciona Flashstart?

Puedes elegir entre 50 categorías y más de 30 subcategorías que tipo de contenido quieres permitir o no. Además también puedes:

- Por defecto bloquea todo tipo de malware
- Lista blanca/negra de dominios siempre permitidos/bloqueados
- Bloqueo por Geolocalización (bloquea un país o continente)



¿Cómo funciona Flashstart?



¿Cómo funciona Flashstart?

```
C:\>nslookup xxx.com 185.236.104.104
Servidor: host-pool-185-236-104-104.flashstart.com
Address: 185.236.104.104

Nombre: xxx.com
Address: 185.236.104.104
```

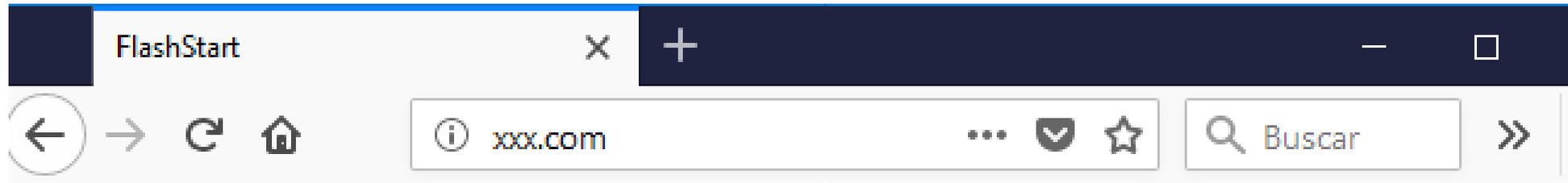
```
C:\>nslookup xxx.com 8.8.8.8
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
Nombre: xxx.com
Address: 141.0.173.173
```

Observa estas 2 consultas de DNS, la IP que devuelve la consulta son distintas.



¿Cómo funciona Flashstart?



A screenshot of a MikroTik access denied page. The top left features the MikroTik logo. To its right is a red button with the text "Acceso Denegado". Below the logo is the EcaTel SRL logo, which consists of a blue cloud with circuit lines and the text "EcaTel SRL". To the right of the EcaTel logo, the text "Ecatel SRL" is displayed in orange, followed by "¡Acceso denegado!" in bold orange. Below this, there are two orange bullet points: "▶ Sitio web prohibido : xxx.com" and "▶ Motivo: Lista negra de sitio web". At the bottom, there are two orange links: "Solicitar desbloquear" and "Informar error de programación", separated by a vertical line.



Flashstart

Es un servicio de pago, encontrarás varias soluciones similares gratuitas y de pago.

Flashstart tiene precios muy económicos desde 50 USD anuales para proteger toda una red.



¿Cómo funciona el bloqueo de Malware?



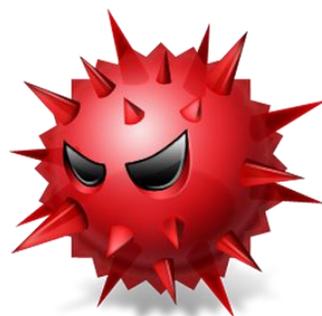
Cuando intentas ingresar a un sitio que contiene malware, Flashstart no te devuelve la IP original del sitio, te devuelve la IP propia de ellos y te muestra un mensaje que el acceso fue bloqueado.



El Ransomware suele utilizar en el correo electrónico un enlace. Los filtros en DNS identifican los dominios maliciosos y bloquean las peticiones, evitando de esta manera la descarga de malware



FlashStart INTERNET PROTECTION



Los antivirus necesitan esperar a que el malware llegue a la PC para detectarlo. Al ejecutar la seguridad en la capa de DNS, se detienen las amenazas antes de que lleguen a los dispositivos finales.

La protección en la capa DNS se extiende a todos los dispositivos conectados a la red (smartphone, tablet, PC's)

La seguridad a nivel de DNS es realmente la capa de seguridad más fácil y rápida de implementar.



¿Cómo funciona el bloqueo de las categorías seleccionadas?

Si bloqueas el acceso a Redes Sociales, cuando intentas ingresar a un sitio de red social como facebook, Flashstart no te devuelve la IP original del sitio, te devuelve la IP propia de ellos y te muestra un mensaje que el acceso fue bloqueado.



Google SafeSearch



puede forzar de manera transparente para que todos los dispositivos de tu red tengan activado el Safesearch.

Nunca tendrás que manipular el dispositivo del usuario final. Lo harás mediante el DNS



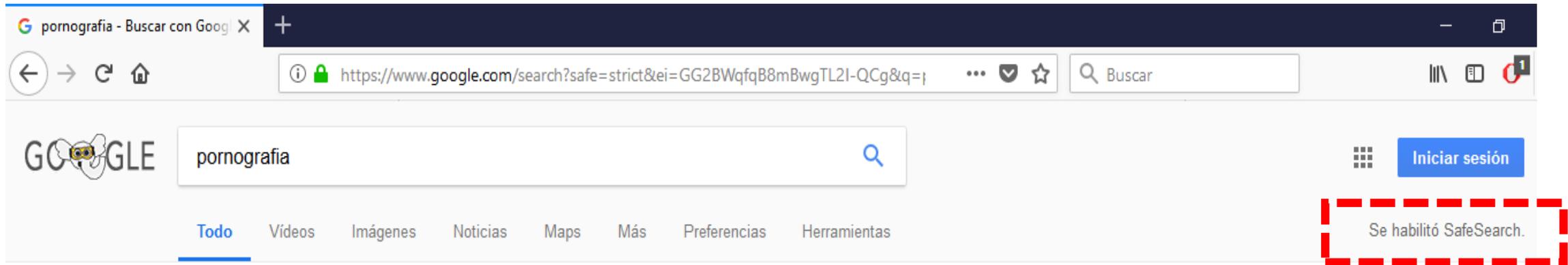
Google SafeSearch

Permite filtrar resultados de la búsqueda en Google, elimina resultados de contenido pornográfico.

Cuando SafeSearch está activado, permite bloquear imágenes, videos y sitios web explícitos de los resultados de la Búsqueda de Google.



Google SafeSearch



The screenshot shows a Google search page for the term "pornografía". The search bar contains the word "pornografía" and a magnifying glass icon. Below the search bar, there are navigation tabs: "Todo" (selected), "Videos", "Imágenes", "Noticias", "Maps", "Más", "Preferencias", and "Herramientas". In the top right corner, there is a blue button labeled "Iniciar sesión". A red dashed box highlights a notification in the bottom right corner that reads "Se habilitó SafeSearch." The browser's address bar shows the URL: "https://www.google.com/search?safe=strict&ei=GG2BWqfqB8mBwgTL2I-QCg&q=pornografía".

Cerca de 20.400.000 resultados (0,26 segundos)

Esto es lo que la pornografía le hace a tu cerebro | Telemundo



www.telemundo.com/.../esto-es-lo-que-la-pornografia-le-hace-tu-cer...

24 mar. 2017

Las relaciones sexuales liberan en el cerebro una sustancia llamada dopamina, relacionada con el placer y ...

Así es el cerebro de una persona que ve pornografía - Muy Interesante

<https://www.muyinteresante.es/.../asi-es-el-cerebro-de-una-persona-que-ve-pornografi...>

La pornografía sigue siendo un tema controvertido. Experimentos anteriores han confirmado el impacto en el cerebro de la estimulación continua del centro del placer mediante el exceso de contenidos sexuales explícitos. Ahora, diversos estudios profundizan aún más en este tema: ¿qué es lo que hace en nuestro ...

Pornografía



El término pornografía o porno hace referencia a todo aquel material que representa actos sexuales o actos eróticos con el fin de provocar la excitación sexual del receptor. [Wikipedia](#)



PROFILE

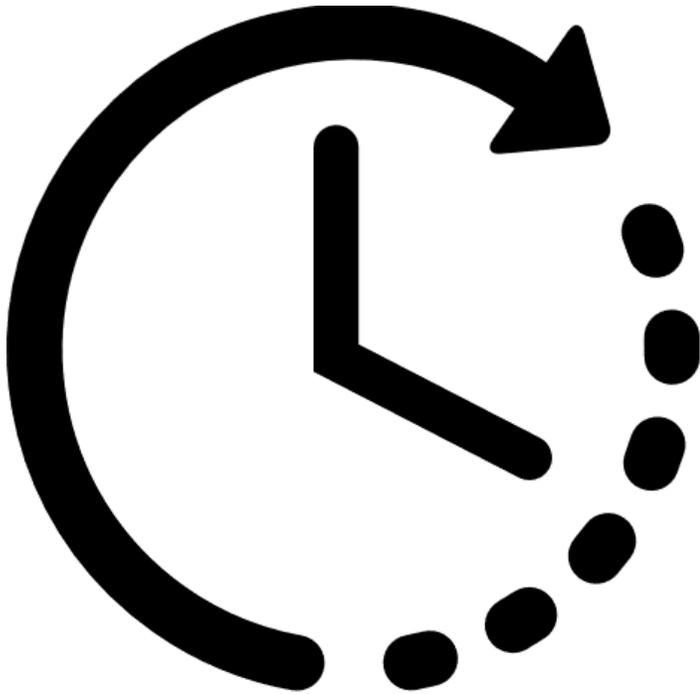
Puedes crear hasta 5 profile (perfiles) por cada IP Publica (red), estos usando diferentes puertos UDP: 53, 110, 143, 5402 y 5403

Ejemplo:

- Perfil sin acceso a la categoría **Redes Sociales**
- Otro perfil con acceso total (Protegiéndolo de **malware**)



Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de DNS
- Como funciona un filtro por DNS
- **Demostración**

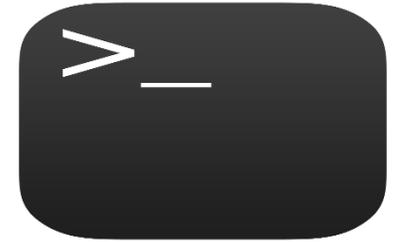




EcaTel SRL

***¡SHOW TIME!
DEMOSTRACION***

COMANDOS



```
/ip firewall address-list
```

```
add address=192.168.88.251 list=DNS_PorDefecto
```

```
add address=192.168.88.252 list=DNS_SinRRSS
```

```
add address=192.168.88.251 list=DNS_IncluyeSoloYoutube
```

```
/ip firewall nat
```

```
add action=accept chain=dstnat comment="Por Defecto" \  
dst-port=53 protocol=udp src-address-list=DNS_PorDefecto
```

```
add action=dst-nat chain=dstnat comment="Solo Youtube" \  
dst-port=53 protocol=udp src-address-list=DNS_IncluyeSoloYoutube \  
to-addresses=185.236.104.104 to-ports=143
```

```
add action=dst-nat chain=dstnat comment="Sin RRSS" \  
dst-port=53 protocol=udp src-address-list=DNS_SinRRSS \  
to-addresses=185.236.104.104 to-ports=110
```

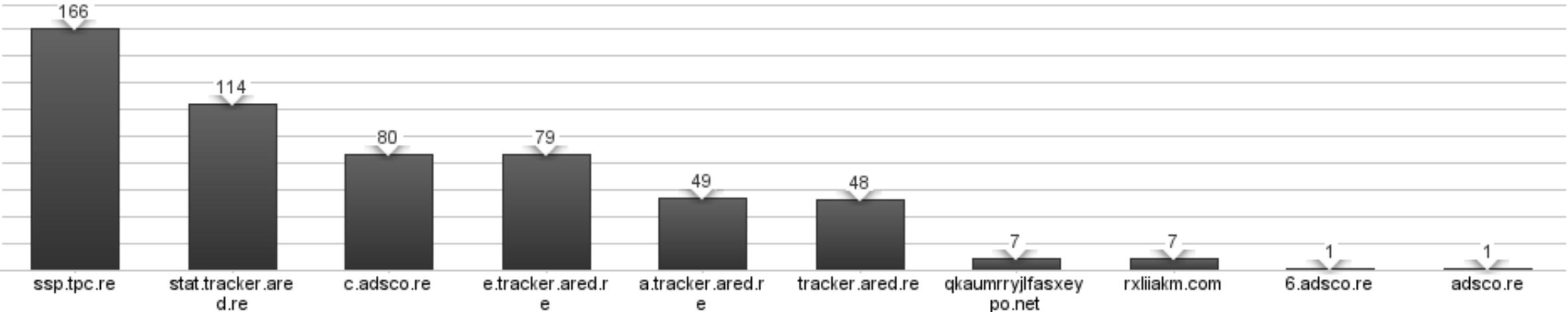


REPORTES



Malware: servidor infectado bloqueado

[\[mas información\]](#)

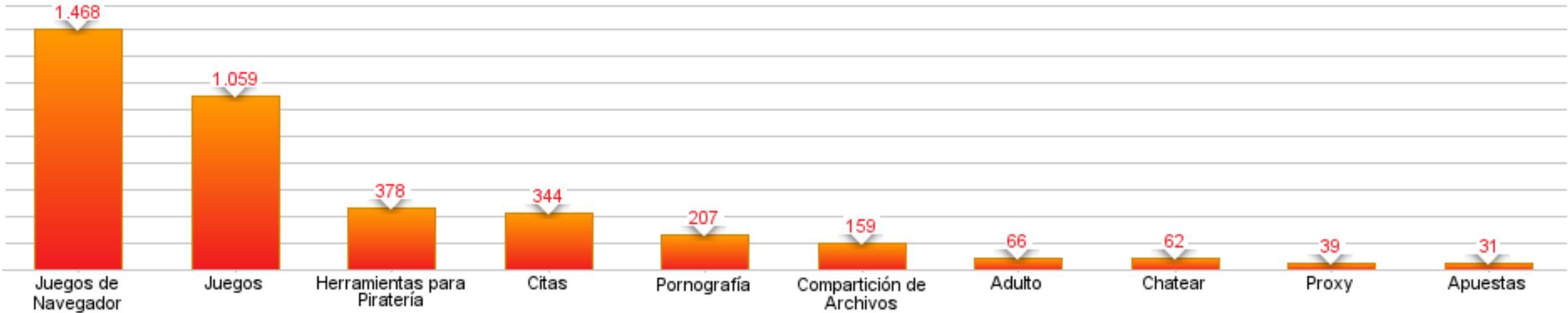


REPORTES



Bloqueadas no deseadas

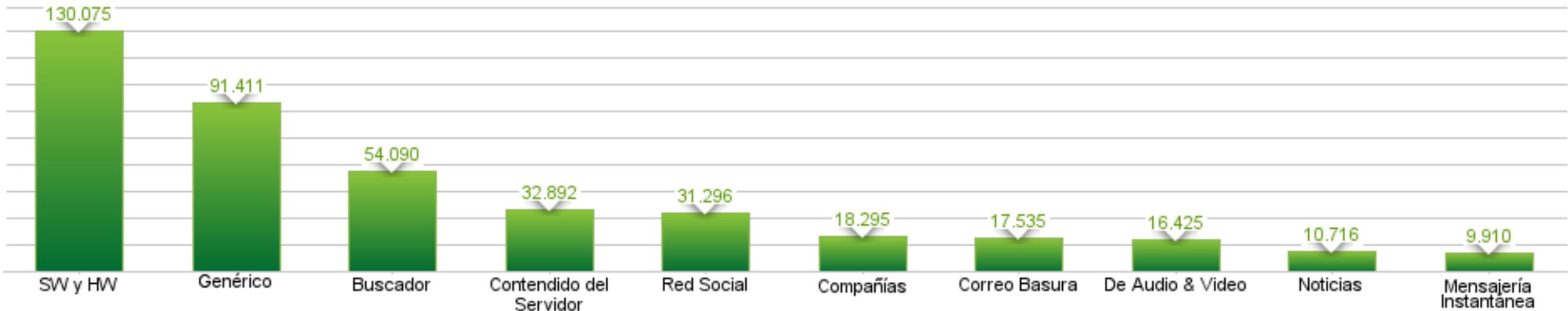
[mas información]



REPORTES

 Permitidas por categoría

[\[mas información\]](#)





MERCADOWISP MEXICO

Solicita en nuestro Stand

GRATIS
Una licencia por 3 meses



FlashStart®
cloud

FlashStart is an advanced, easy to use, **Web filter** requiring **no additional hardware**. Just configure your router and **enjoy safe surfing!**

 Stop strains of Ransomware Malware	 Remove time-wasting games etc	 Filter offensive materials (porn, terrorism)	 Few mins to set-up
--	---	--	--

GH5KU8N2PJ

Activate now on your device: **90 free days**
Register now at <http://cloud.flashstart.com/>
If you are a Dealer, select "Reseller" during first registration.



¡Se Reseller!

- » **Genera cuentas DEMO para tus potenciales clientes**
- » **Instala el filtro en tus routers MikroTik**




MERCADOWISPMEXICO





MERCADOWISP
MEXICO

¡Gracias!

FlashStart®

INTERNET PROTECTION

partner

¿PREGUNTAS?