MUM – Mexico 2018
Filtrado por DNS

Por: Ing. José Miguel Cabrera
Ecatel SRL

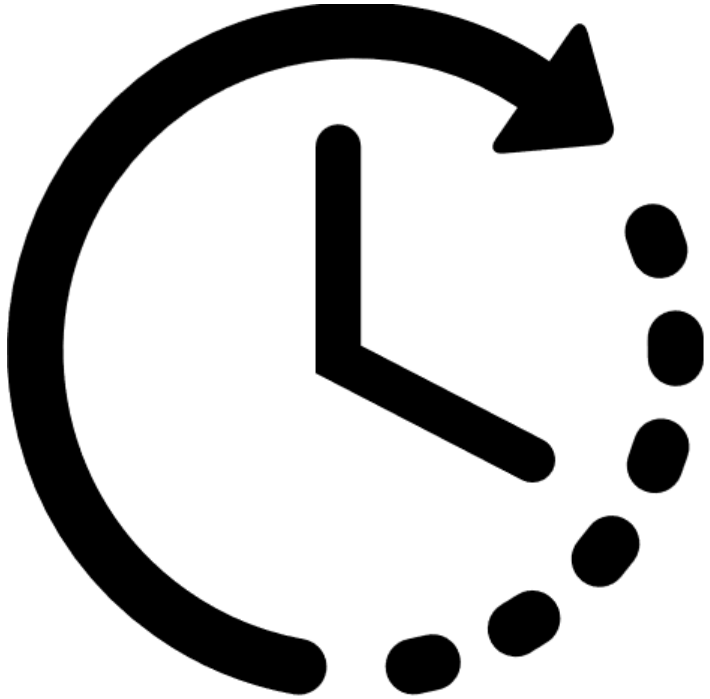
MikroTik CERTIFIED TRAINER

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

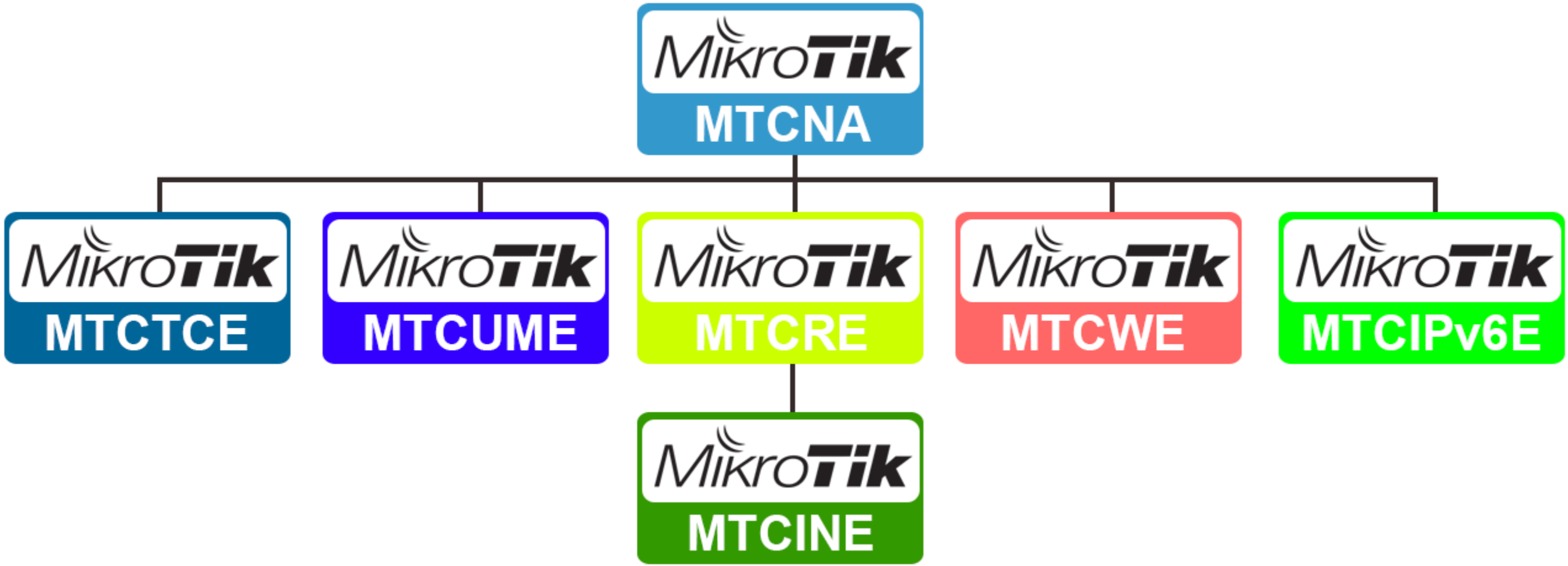
Certificaciones:

- **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

MikroTik TRAINING CENTER

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

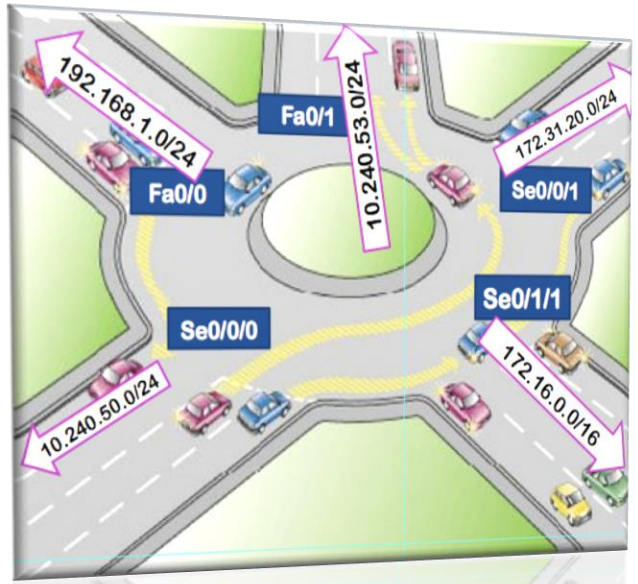
- Capitulo 1: Introducción
- Capitulo 2:DHCP
- Capitulo 3:Bridging
- Capitulo 4:Routing
- Capitulo 5:Wireless
- Capitulo 6:Firewall
- Capitulo 7:QoS
- Capitulo 8:Tuneles VPN
- Capitulo 9:Herramientas

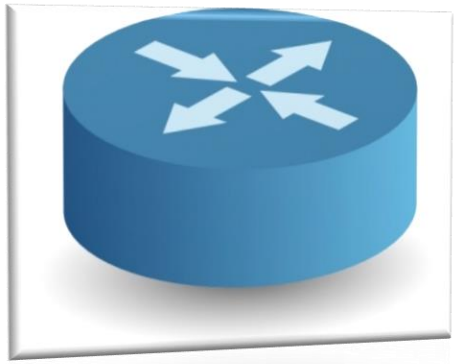
Objetivos Del Curso MTCRE

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



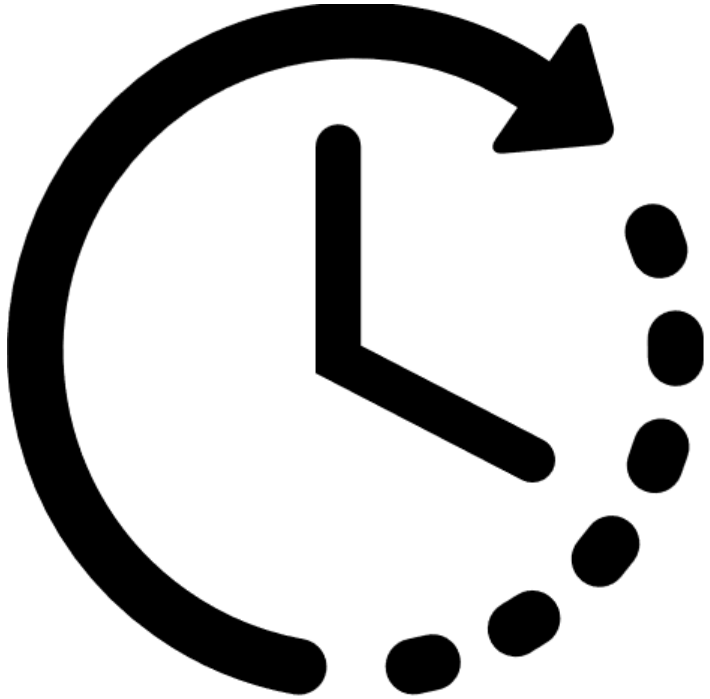


- **Capitulo 3:** Enrutamiento InterVLAN y VPN
- **Capitulo 4:** Ennrutamiento Dinamico (OSPF)

MERCADOWISPMEXICO

GRATIS
Participa de una rifa de becas para cursos
https://ecatel.com.mx/formmx

Scheduler



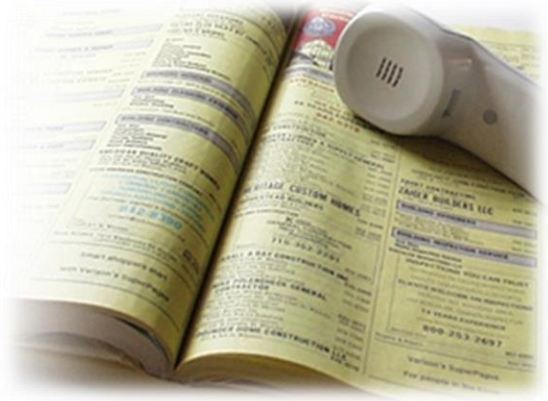
- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- **Conceptos de DNS**
- Como funciona un filtro por DNS
- Demostración

DNS

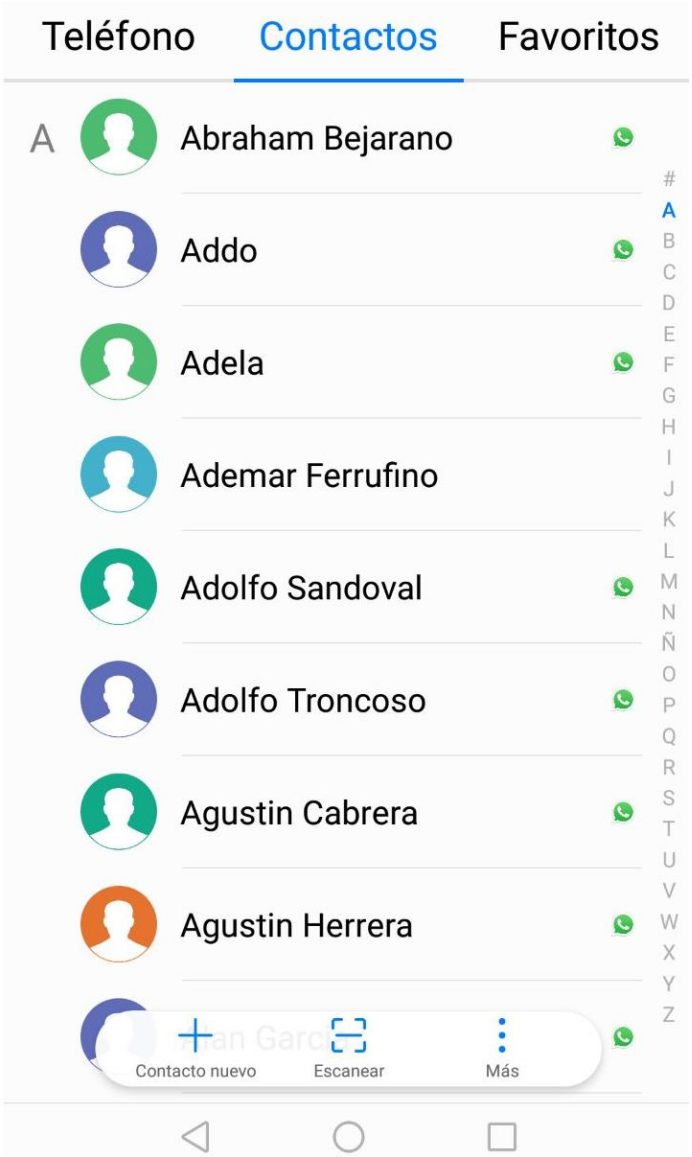
DNS (Domain Name System - Sistema de nombres de dominio) es un protocolo que convierte nombres de dominio a direcciones IP.

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)

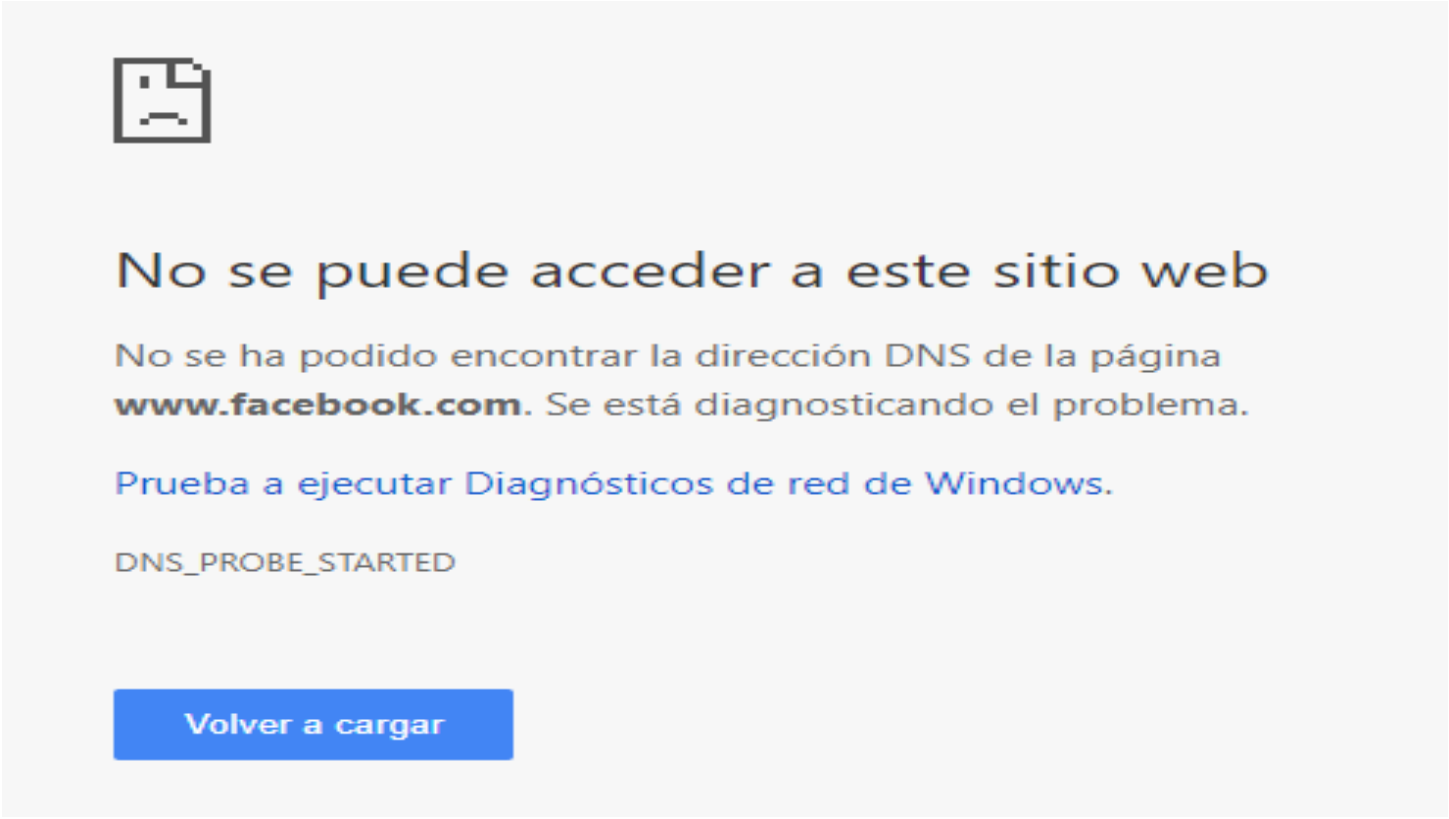
de cualquier IP. Solamente desde sus clientes.

¿Qué pasa cuando balanceo 2 conexiones de

Internet de distintos proveedores?

Problema con el DNS

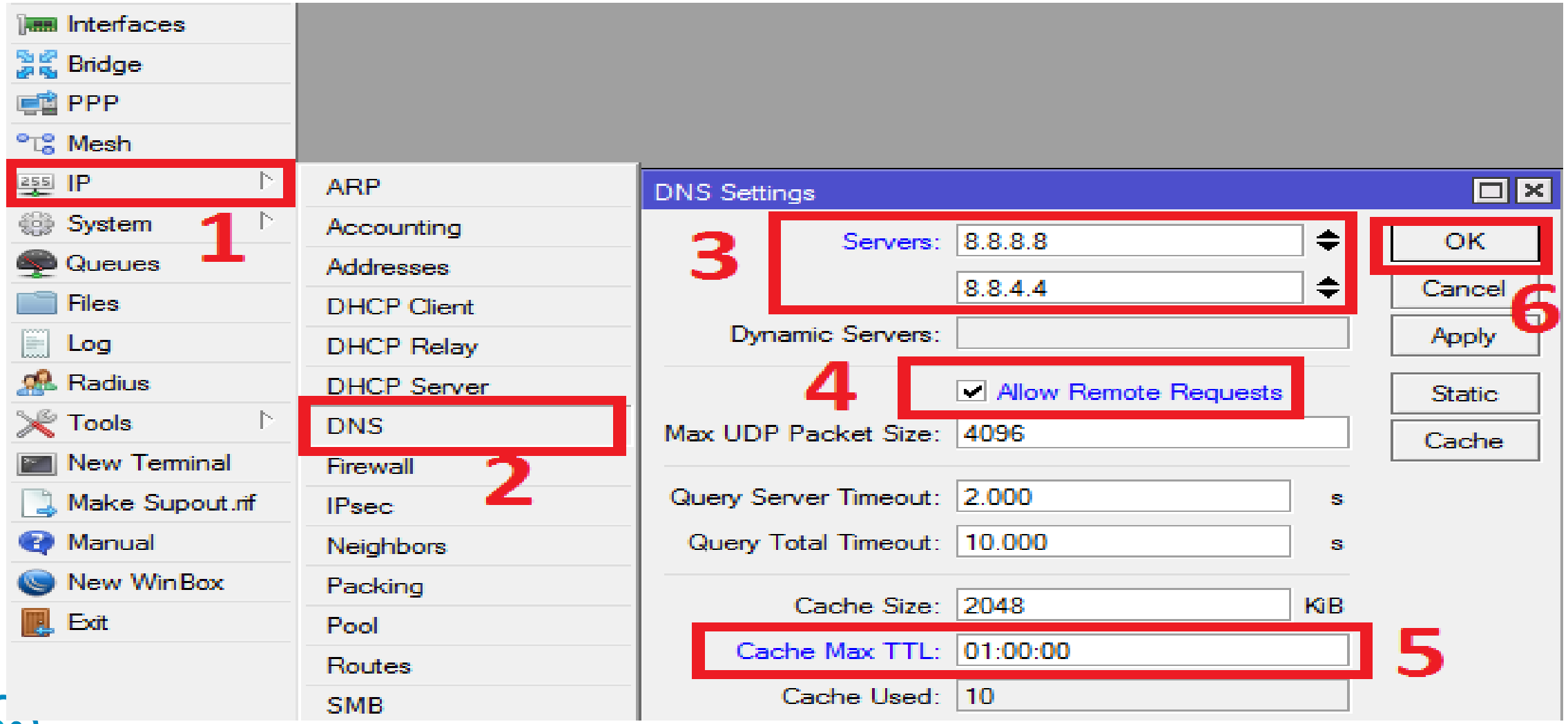
Entonces algunas consultas DNS serán rechazadas y nuestro navegador mostrará



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



ADVERTENCIA

- Proteja su router, **NO** permita las consultas desde redes externas (Internet). Con una regla de Firewall Filter haga DROP al trafico 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 (pudiera 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

Amplificacion

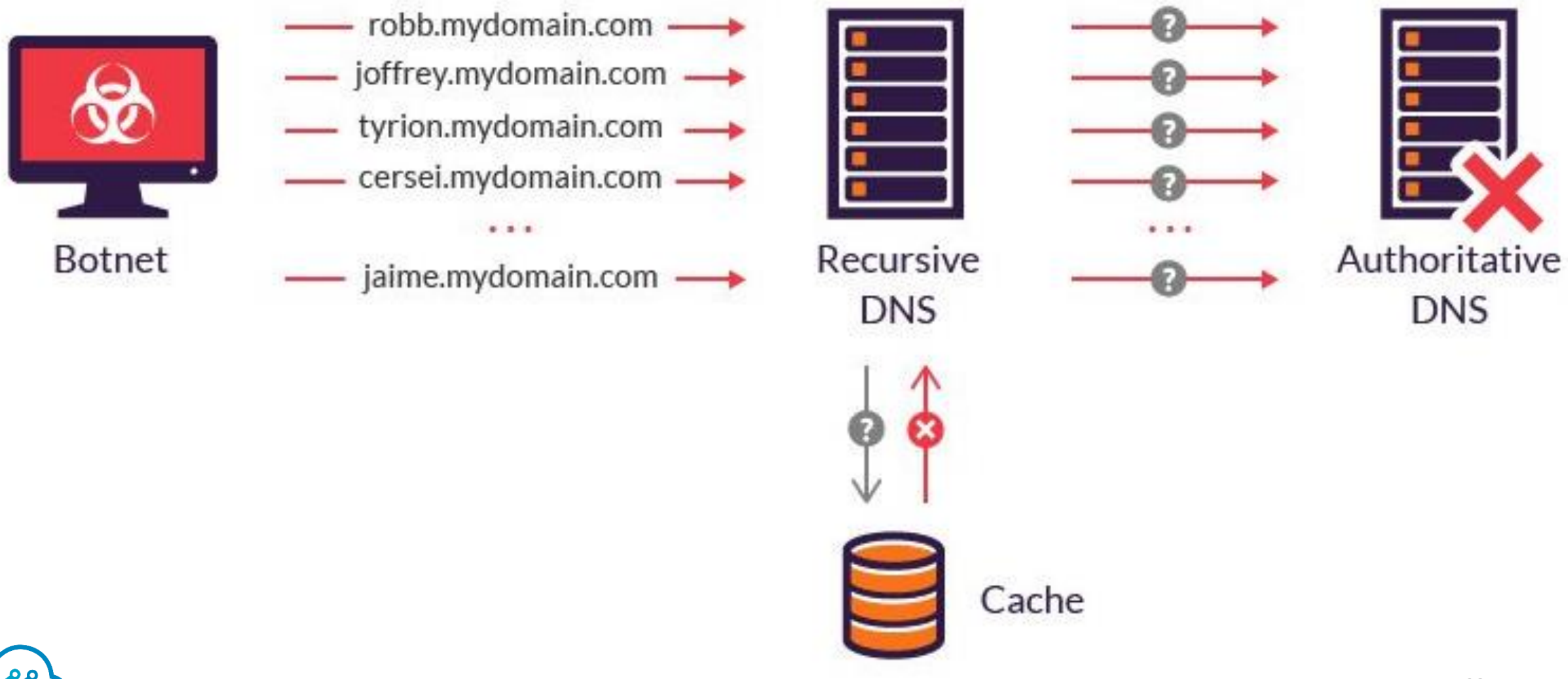
Ataque de amplificación de DNS, es un ataque DDoS asimétrico. Supongamos que la victima (otro DNS Server) tiene la IP 1.2.3.4 el atacante envía una pequeña consulta DNS con una IP de origen falsa (la de su victima), haciendo que las respuestas vayan hacia la victima. Con estos ataques, el objetivo del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

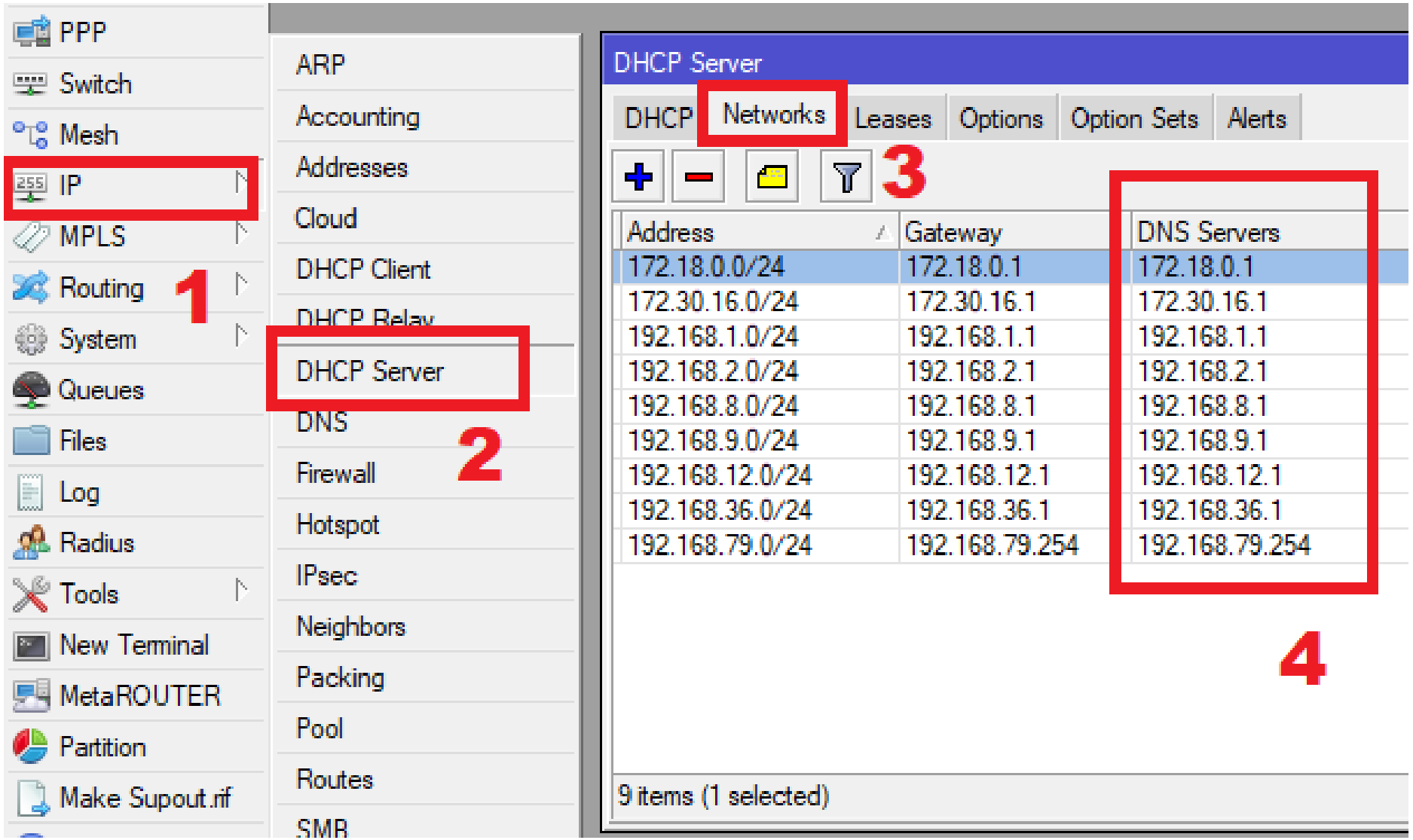


Aplicar DNS

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



DNS Transparente

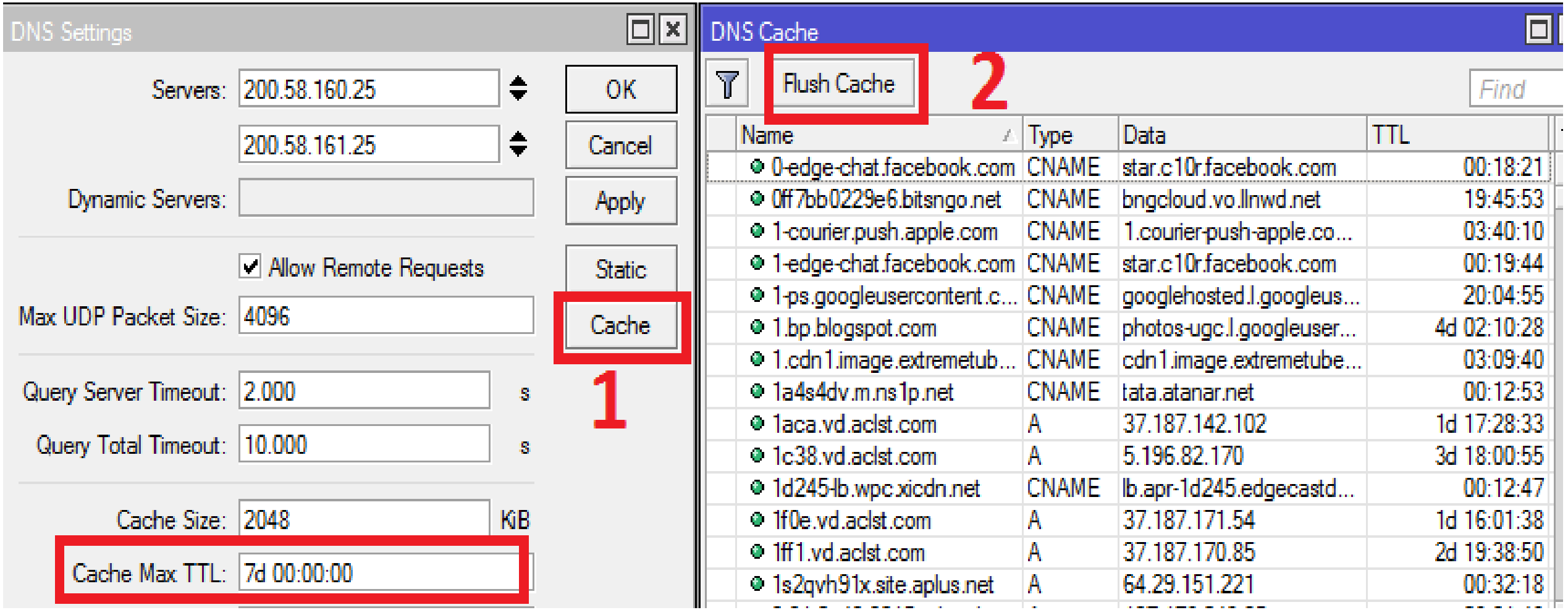
Debes aplicar el siguiente comando:

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

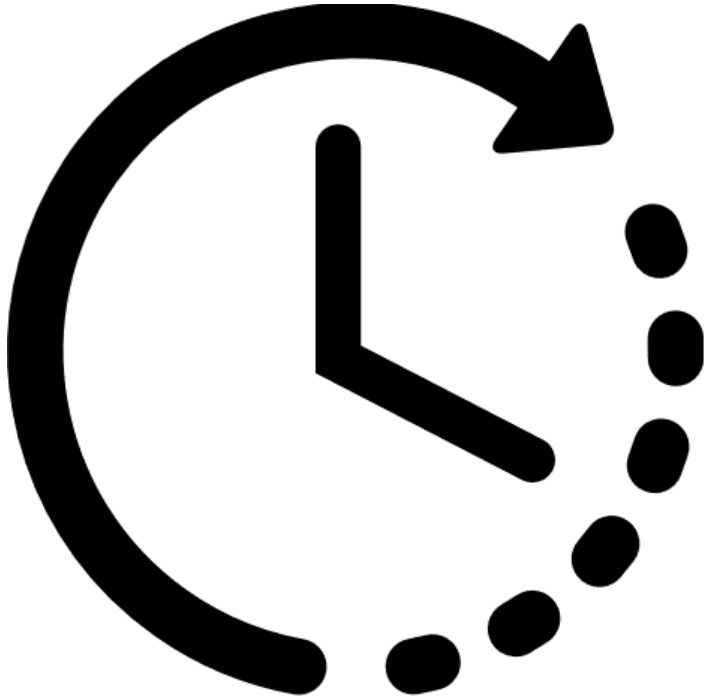
¿Por qué ambos?

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



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

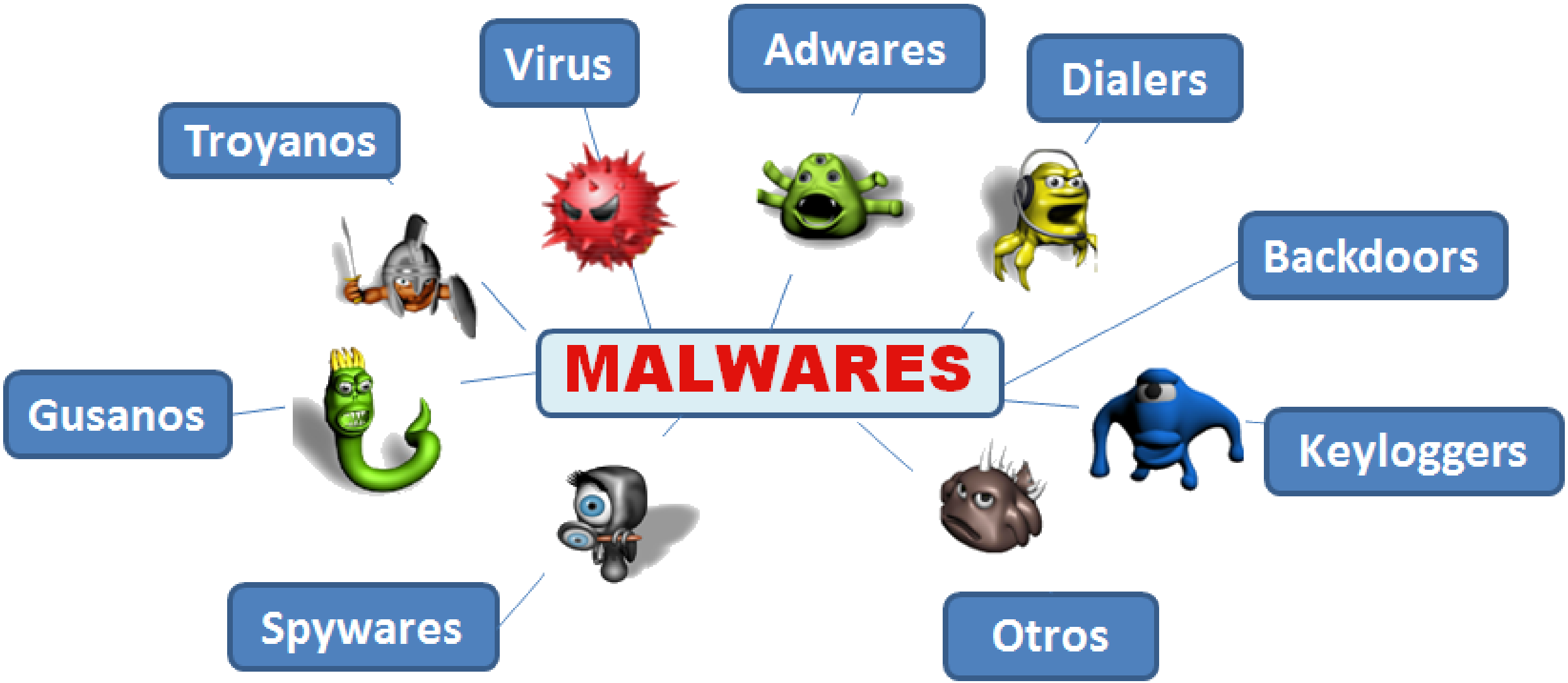
En la actualidad las fuentes más populares de infección de malware son:

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

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 extraibles



¿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 subcategorias en el Blacklist
- **Detiene más de 250 000 sitios que contienen Malware**

Flash Start INTERNET PROTECTION

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.

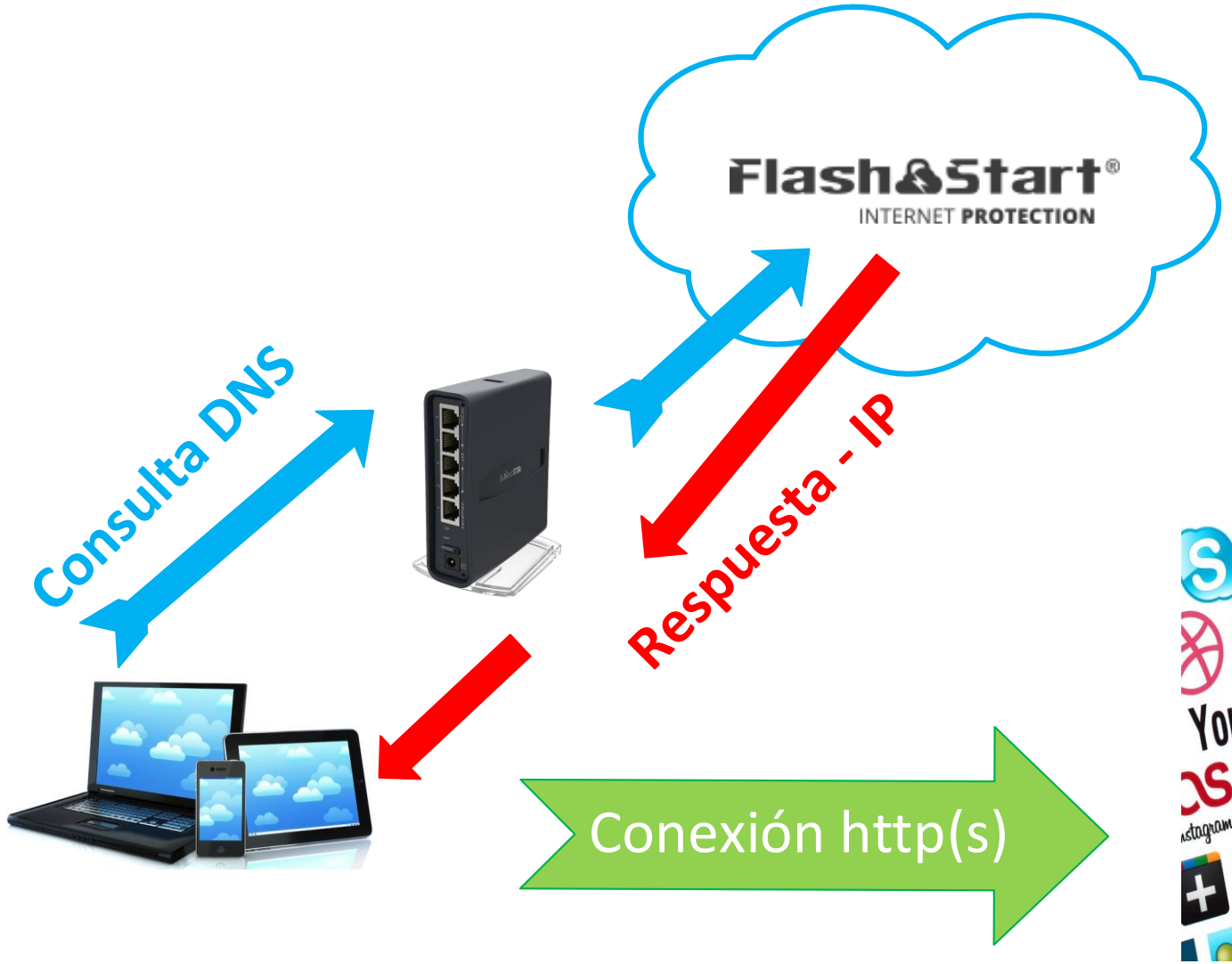
http://www.flashstart.com/

¿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 Geolocalizacion (bloquea un país o continente)

¿Cómo funciona Flashstart?



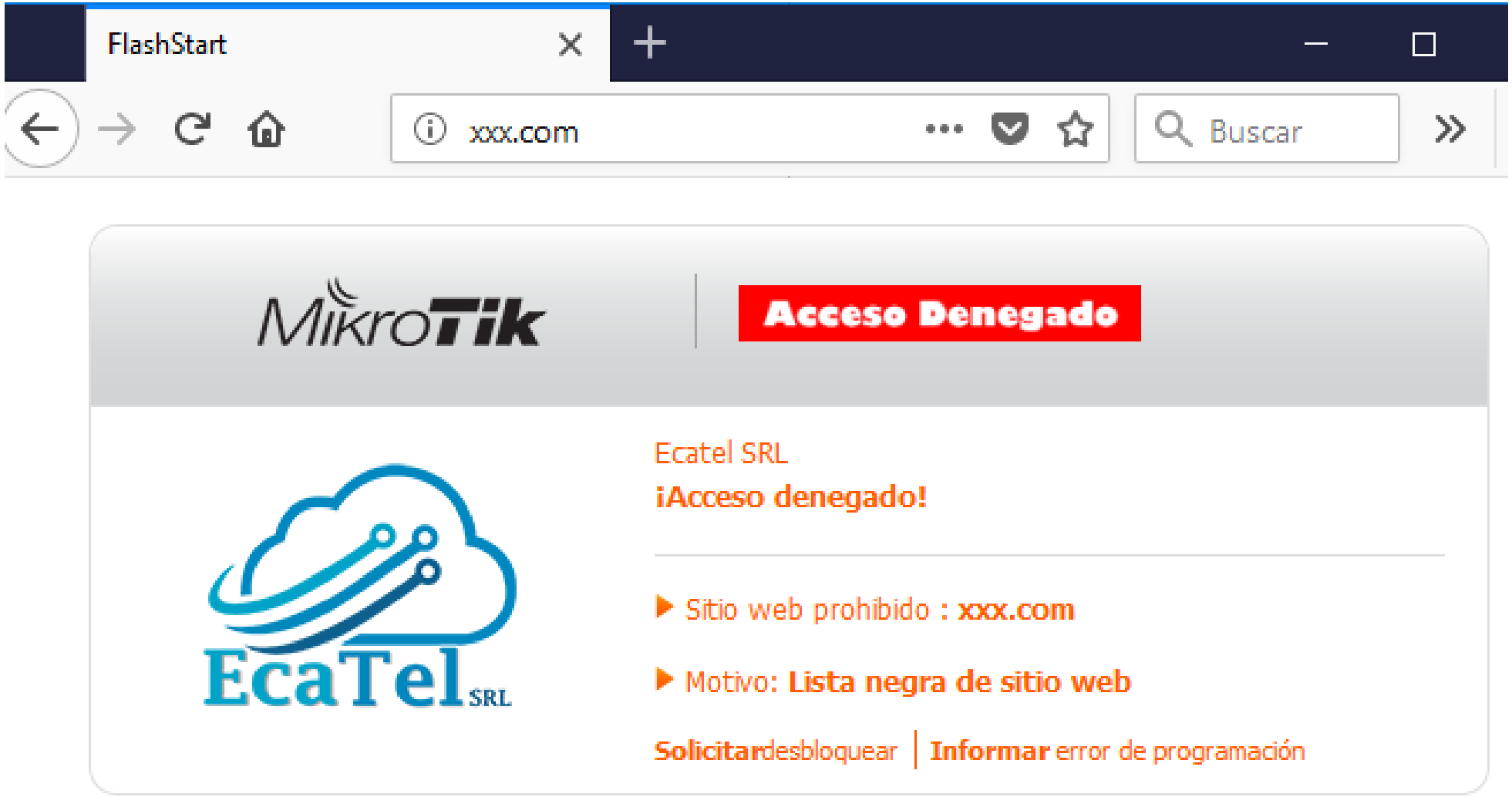
¿Cómo funciona Flashstart?

```
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?



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.

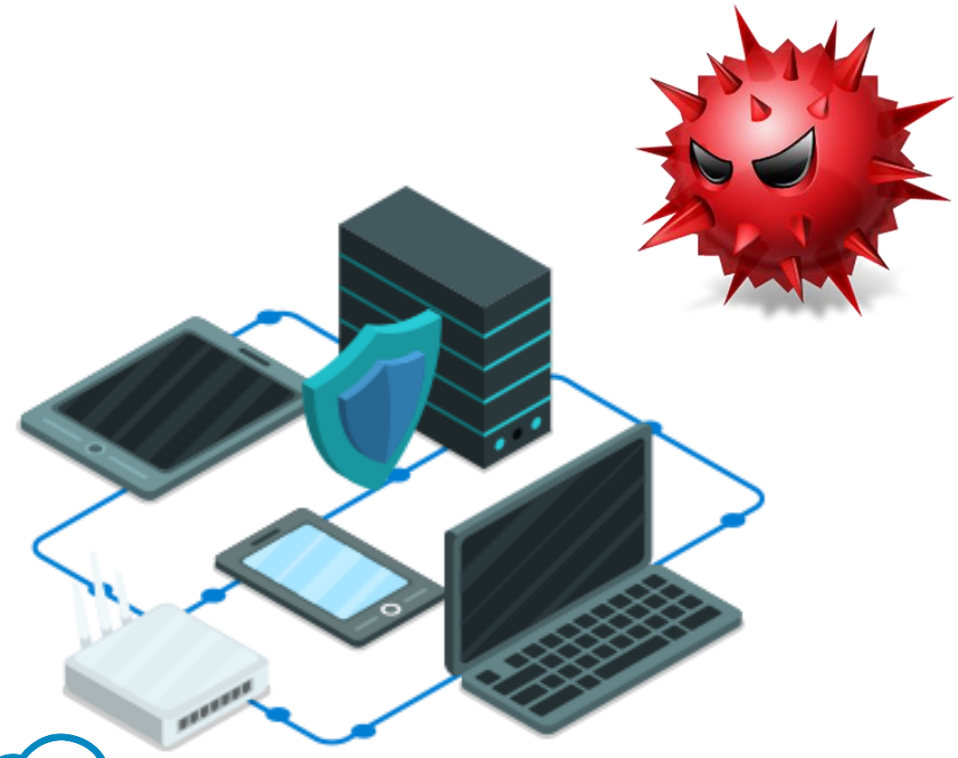
¿Cómo funciona el bloqueo de Malware?

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

EcaTel SRL

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

Flash&Start® INTERNET PROTECTION puede forzar de manera transparente para que todos los dispositivos de tu red tengan activado el Safesearch.

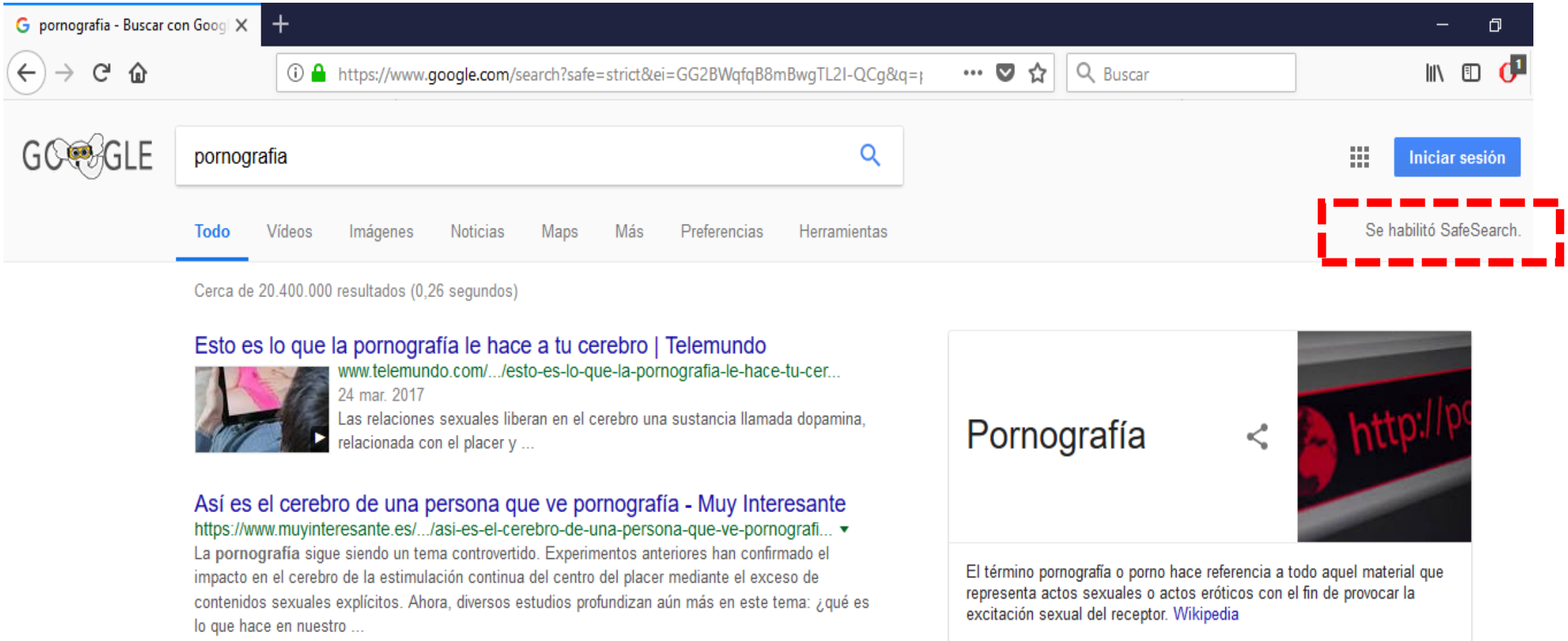
Nunca tendrás que manipular el dispositivo del usuario final. Lo harás mediante el DNS

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



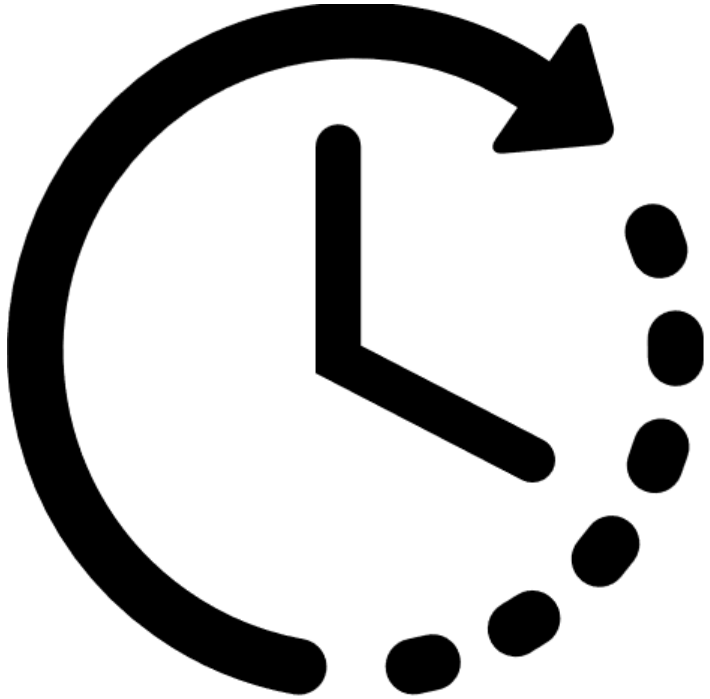
PROFILE

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

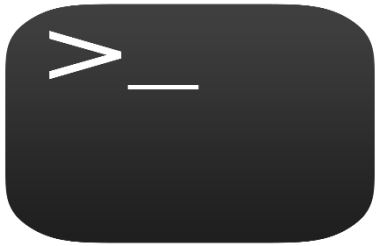


- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de DNS
- Como funciona un filtro por DNS
- **Demostración**

EcaTel SRL

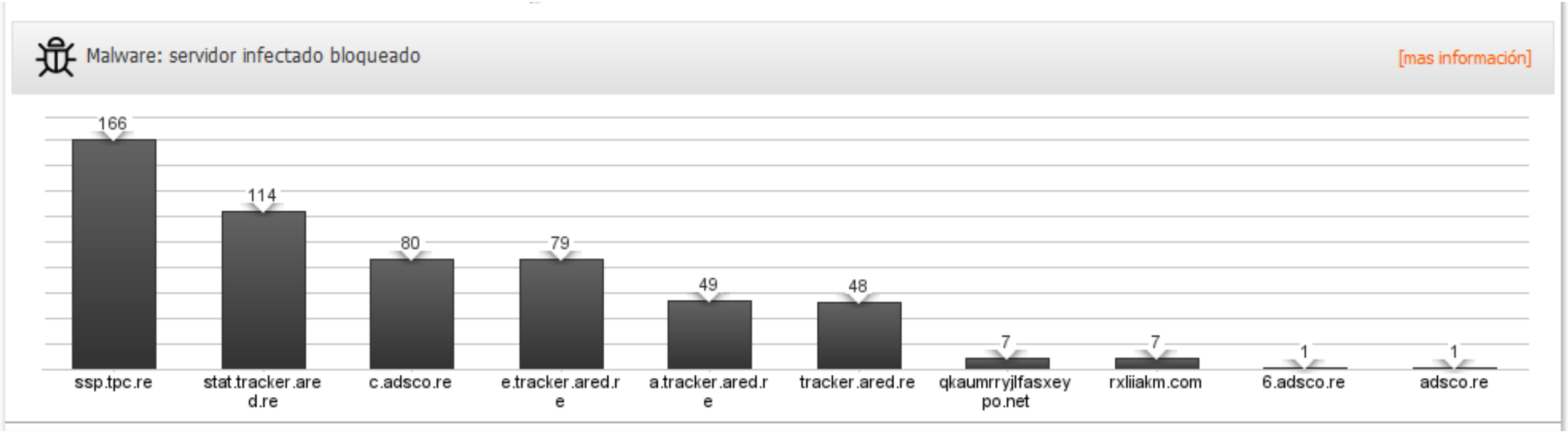
¡SHOW TIME!
DEMOSTRACION

COMANDOS

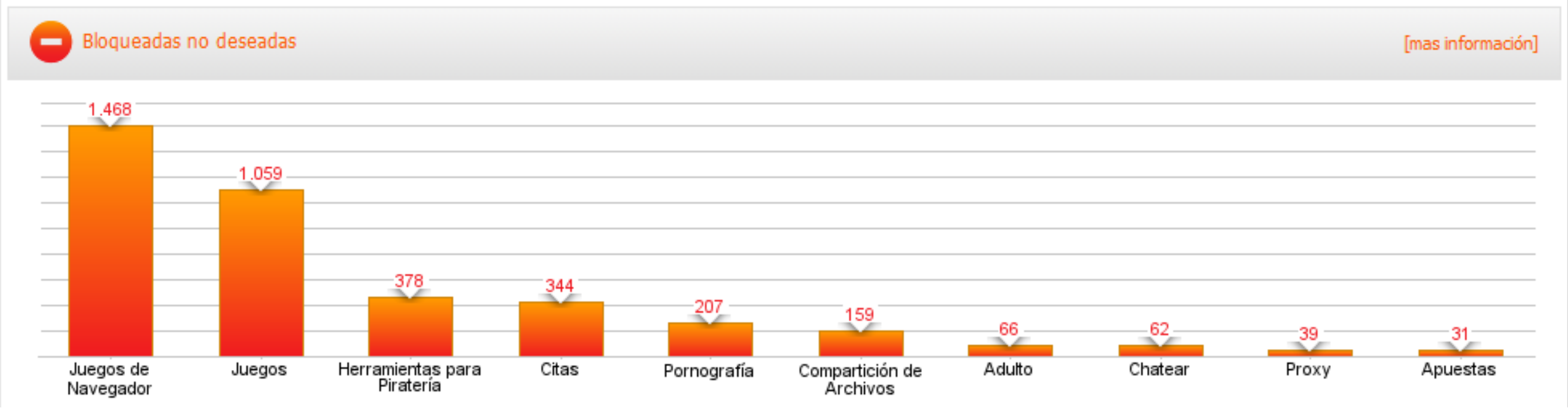



```
/ip firewall address-list
add address=192.168.88.251 list=DNS_PorDefecto
add address=192.168.88.252 list=DNS_SinRRSS
add address=192.168.88.251 list=DNS_IncluyeSoloYoutube

/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
```

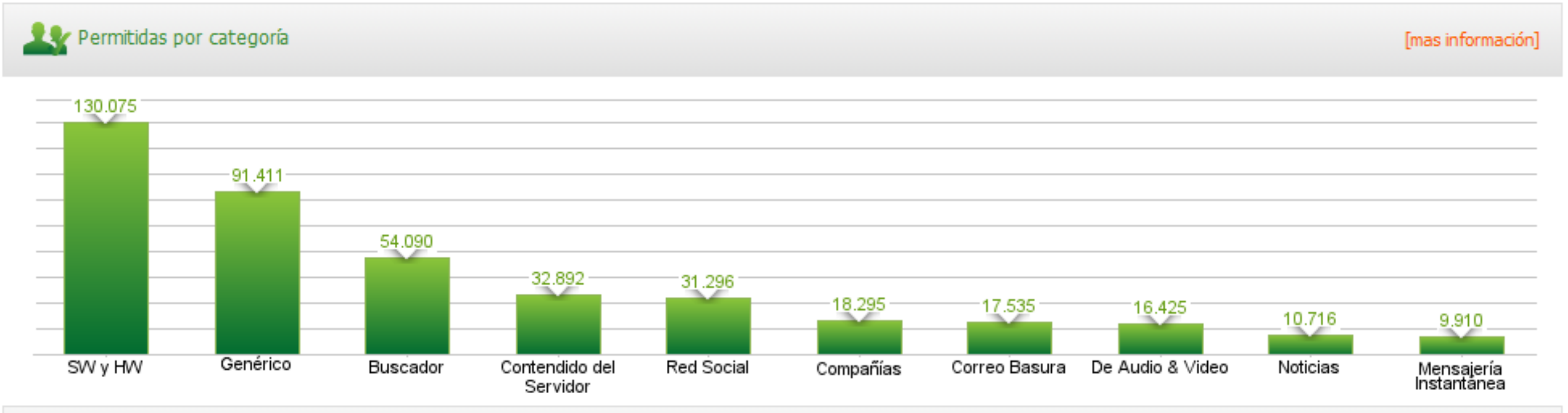
REPORTES



REPORTES



REPORTES



MERCADOWISPMEXICO

Solicita en nuestro Stand

GRATIS
Una licencia por 3 meses

¡Se Reseller!

» **Genera cuentas DEMO para tus potenciales clientes**

» Instala el filtro en tus routers MikroTik

MERCADOWISPMEXICO

EcaTel SRL

MERCADOWISPMEXICO

¡Gracias!

FlashStart®
INTERNET PROTECTION partner

¿PREGUNTAS?