IPCOM SISTEMAS S.A.S.

Manual de Implementación DNS Seguro IPcom

Redirección y control de DNS en MikroTik RouterOS

Guía técnica para ISP clientes del servicio DNS Seguro de IPcom

Versión 1.3 · Agosto de 2026

> **Propósito** Implementar una redirección DNS controlada, verificable y compatible con buenas prácticas de firewall. La guía utiliza RouterOS v7 como referencia; en RouterOS v6 pueden existir diferencias de sintaxis o interfaz.

Contenido

> ***Las capturas del manual son ejemplos de referencia. Nombres de clientes e IP específicas pueden aparecer anonimizados. Cada ISP debe adaptar interfaces, pools y servidores DNS a su topología y a los datos suministrados por IPcom.***

> **Antes de comenzar** Haga una copia de seguridad/export de la configuración y programe una ventana de cambio. Sustituya todos los valores entre < > por datos reales de su red o por las direcciones DNS que IPcom le haya asignado.

1. Objetivo y alcance

Este manual está dirigido a ISP que utilizan el servicio DNS Seguro de IPcom y desean reducir la posibilidad de que los equipos finales evadan la política DNS mediante resolvers externos. El enfoque principal es la redirección de DNS clásico (UDP/TCP 53) y las condiciones de firewall necesarias para que dicha redirección sea estable, segura y fácil de auditar. También presenta el valor de la redirección DNS como soporte para el cumplimiento de políticas de bloqueo aplicables y como medida preventiva para reducir exposición a abuso que pueda afectar la reputación de las IP del ISP.

> **Alcance deliberado** No es un manual general de seguridad MikroTik. Las recomendaciones de firewall incluidas son las mínimas que apoyan una implementación DNS robusta; cada ISP debe conservar sus propias políticas de acceso, gestión, routing y servicios.

2. ¿Por qué DNS Seguro de IPcom?

DNS Seguro de IPcom añade una capa preventiva de seguridad en la etapa de resolución de nombres. El servicio integra fuentes y listas de inteligencia de amenazas para bloquear grandes volúmenes de dominios e indicadores asociados con phishing, malware, botnets, spam y otras amenazas conocidas.

Cuando un dispositivo intenta resolver un dominio identificado como malicioso, la política DNS puede impedir la resolución antes de que se establezca una comunicación útil con el destino. Esto amplía la protección hacia los dispositivos finales sin exigir software adicional en cada equipo.

2.1 Bloqueos regulatorios solicitados a los ISP

DNS Seguro de IPcom incorpora de forma centralizada los listados de dominios y hosts asociados a URLs cuya restricción ha sido solicitada a los ISP por MinTIC y otras autoridades competentes en Colombia. Esto permite que el operador aplique la política de bloqueo a través de la capa DNS sin cargar miles de reglas individuales en el firewall del router.

Dentro de las categorías operativas se contemplan, entre otras, listados de Coljuegos, material de abuso sexual infantil, dominios asociados a servicios de streaming ilegal como Magis TV y órdenes judiciales o administrativas. IPcom mantiene información operativa y de consulta en https://bloqueos-isp-mintic.com/ y https://bloqueos-isp-mintic.com/dns/. Las zonas de política se actualizan de forma centralizada para los clientes del servicio.

> ***Precisión técnica: DNS puede bloquear el dominio o hostname asociado a una URL. Si una orden exige diferenciar rutas específicas dentro del mismo dominio (por ejemplo, /ruta/archivo), se requieren controles adicionales de capa de aplicación.***

2.2 Menor exposición a abuso, spam y problemas de reputación IP

El filtrado de dominios asociados con malware, botnets, phishing, spam y otras fuentes de abuso también aporta un beneficio operativo al ISP. Al reducir la probabilidad de que equipos comprometidos contacten infraestructura maliciosa, participen en campañas automatizadas o generen tráfico abusivo, disminuye la exposición de las direcciones IP del operador a incidentes que pueden afectar su reputación.

Esto puede ayudar a reducir uno de los problemas más costosos para un ISP: la aparición de direcciones o prefijos en listas de reputación o listas negras utilizadas por servicios de correo, plataformas de seguridad y redes remotas. DNS Seguro de IPcom no garantiza por sí solo que una IP nunca sea listada, pero constituye una capa preventiva que complementa controles como firewall, antispam, monitoreo de abuso, rate limits y gestión de clientes comprometidos.

Beneficio para el ISP: menos tráfico hacia infraestructura maliciosa, menor probabilidad de abuso originado desde clientes infectados y una postura preventiva que ayuda a proteger la reputación de las IP públicas del operador.

Precisión técnica El DNS seguro complementa al firewall y a las soluciones de endpoint; no los sustituye. Aunque opera sobre una función de aplicación y ayuda a frenar amenazas antes de la conexión, no debe describirse como un firewall de capa 7 completo.

Beneficio	Efecto operativo	Valor para el ISP
Bloqueo temprano	Impide resolver dominios conocidos como maliciosos	Reduce exposición antes de establecer sesiones
Cobertura centralizada	La política se aplica en el resolver	Protege múltiples tipos de dispositivos
Menos dependencia del usuario	No exige configurar cada aplicación	Facilita operación en redes masivas
Trazabilidad	Los eventos DNS pueden medirse y auditarse	Ayuda a soporte y diagnóstico

3. Arquitectura recomendada

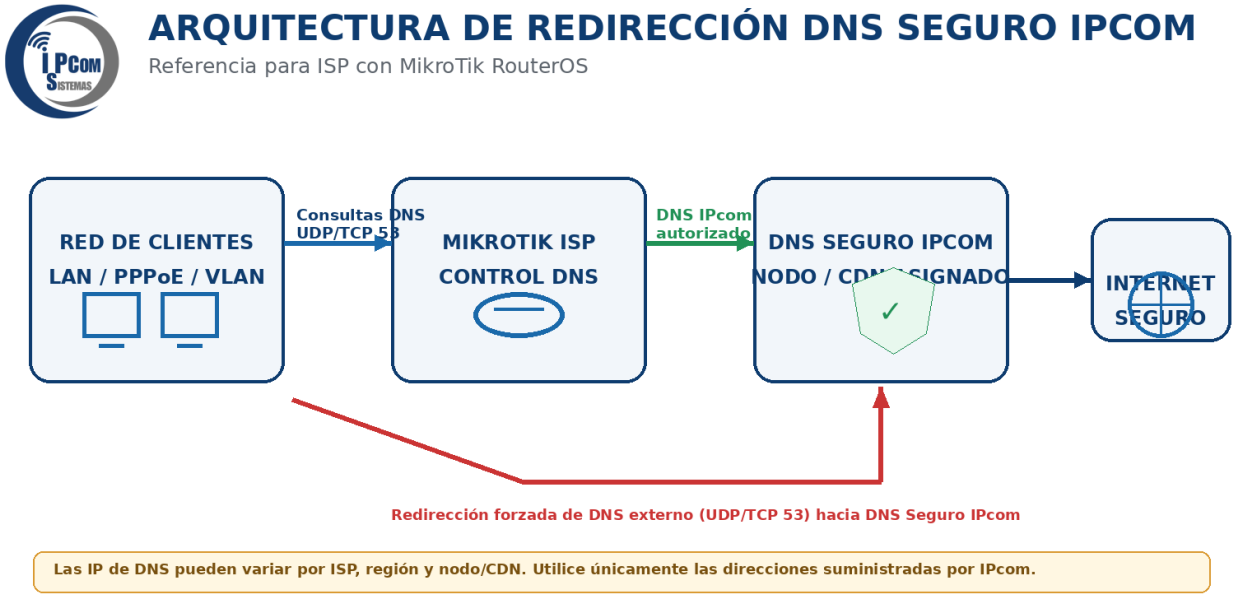

Figura 1. Arquitectura de referencia para redirección hacia DNS Seguro IPcom. Las IP de DNS son asignadas por IPcom según nodo/CDN.

El modelo recomendado utiliza el MikroTik como punto de control. Los DNS autorizados de IPcom se permiten sin alteración; las consultas DNS a otros resolvers se redirigen al resolver local del MikroTik, que a su vez consulta los DNS seguros configurados como upstream.

4. Prerrequisitos y buenas prácticas

4.1 Separar WAN, LAN y clientes

MikroTik permite agrupar interfaces en listas y reutilizarlas en firewall. Para una implementación mantenible se recomienda, como mínimo, diferenciar WAN y LAN. En redes con administración, backhaul o servicios internos, es preferible crear además una lista CLIENTES y aplicar la política DNS únicamente allí.

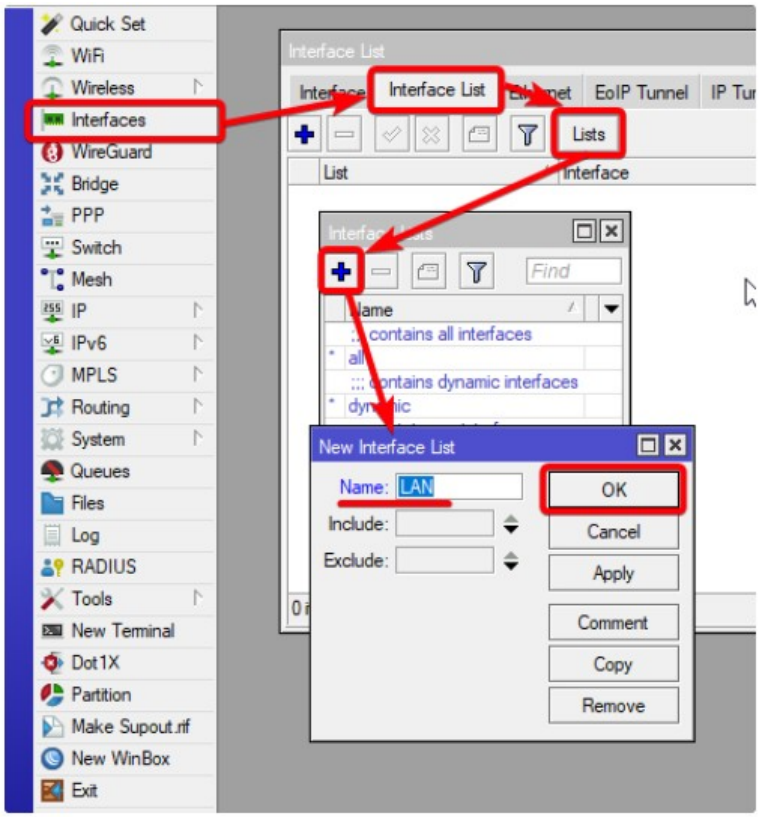

Figura 2. Creación de una Interface List en WinBox. Repita el procedimiento para LAN y WAN.

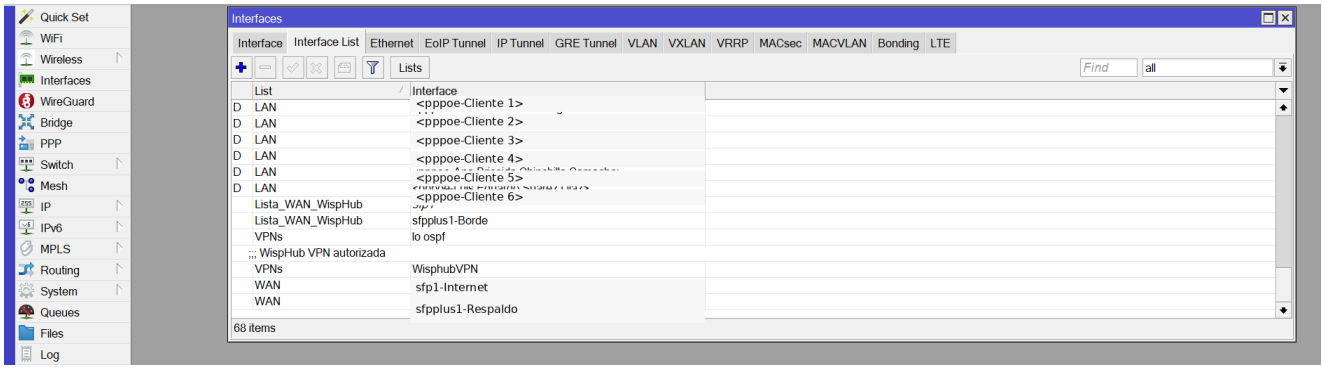

Figura 3. Ejemplo anonimizado de miembros de Interface Lists. Las sesiones/clientes pertenecen a LAN; los enlaces de Internet o tránsito pertenecen a WAN.

Ejemplo de listas de interfaces

```
/interface list
add name=WAN comment="Salidas a Internet"
add name=LAN comment="Redes internas"
add name=CLIENTES comment="Interfaces/redes sujetas a DNS Seguro"

/interface list member
add list=WAN interface=<INTERFAZ_WAN>
add list=LAN interface=<INTERFAZ_LAN>
# Agregue a CLIENTES la interfaz/VLAN de abonados cuando corresponda.
```

> **PPPoE** Si los abonados son PPPoE, la política puede aplicarse con in-interface=all-ppp o mediante una interface-list asignada desde el perfil PPP. Use all-ppp solo cuando todos los PPP deban quedar bajo la misma política; VPN administrativas pueden requerir exclusión.

4.2 Identificar los DNS autorizados

Cree una lista dedicada con las direcciones de DNS Seguro entregadas por IPcom. No mezcle esta lista con resolvers públicos ajenos al servicio.

> ***Importante: las direcciones IP de DNS Seguro pueden variar según el ISP, la región y el nodo/CDN asignado. Utilice únicamente las IP entregadas por IPcom para su servicio y mantenga actualizada la lista DNS-PERMITIDOS.***

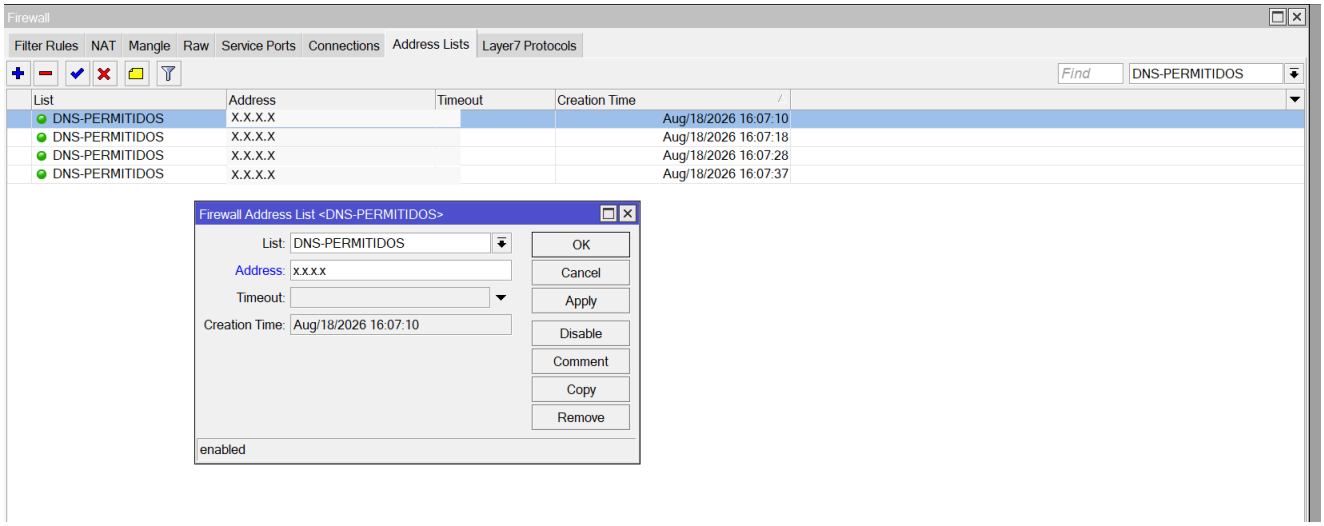

Figura 4. Lista DNS-PERMITIDOS en WinBox. Las IP se muestran ocultas porque cada ISP puede recibir direcciones diferentes según su nodo/CDN.

Lista de DNS autorizados

```
/ip firewall address-list
add list=DNS-PERMITIDOS address=<DNS_IPCOM_1> comment="DNS Seguro IPcom 1"
add list=DNS-PERMITIDOS address=<DNS_IPCOM_2> comment="DNS Seguro IPcom 2"
```

> **Importante** Las direcciones <DNS_IPCOM_1> y <DNS_IPCOM_2> son marcadores. Use únicamente las IP que IPcom haya asignado o confirmado para su servicio.

4.3 Orden lógico del firewall

Zona	Función recomendada	Motivo
RAW	Descartar tráfico evidente no deseado antes de conntrack	Reduce trabajo innecesario
NAT dstnat	Excepciones DNS y luego redirección	El orden define qué consulta se intercepta
FILTER input	Proteger servicios del propio router	Evita convertirlo en resolver abierto
FILTER forward	Controlar tráfico de clientes, incluido DoT	Impide bypass por TCP/853

5. Modelo de implementación

Figura 2. Decisión aplicada a cada consulta DNS clásica.

La lógica es intencionalmente simple: permitir primero los destinos DNS autorizados y redirigir después cualquier otra consulta UDP/TCP 53 originada por clientes. Esta secuencia evita que los resolvers IPcom sean capturados por la regla de redirección.

6. Configuración paso a paso en MikroTik

6.1 Configurar el resolver del MikroTik

Resolver local usando DNS Seguro IPcom

```
/ip dns
set servers=<DNS_IPCOM_1>,<DNS_IPCOM_2> allow-remote-requests=yes
```

> **Seguridad** allow-remote-requests=yes solo debe usarse junto con reglas de INPUT/RAW que impidan consultas DNS desde Internet. El objetivo es atender a los clientes autorizados, no publicar un resolver abierto.

6.2 Dimensionamiento recomendado de DNS Settings

Cuando la redirección utiliza action=redirect, el MikroTik recibe las consultas DNS de los clientes y las reenvía hacia DNS Seguro de IPcom. Por ello, /ip dns debe dimensionarse de acuerdo con la cantidad de clientes y la concurrencia real. MikroTik documenta cache-size, max-concurrent-queries y max-concurrent-tcp-sessions como límites configurables; los valores siguientes son una recomendación operativa de IPcom y deben validarse contra RAM, CPU y carga real.

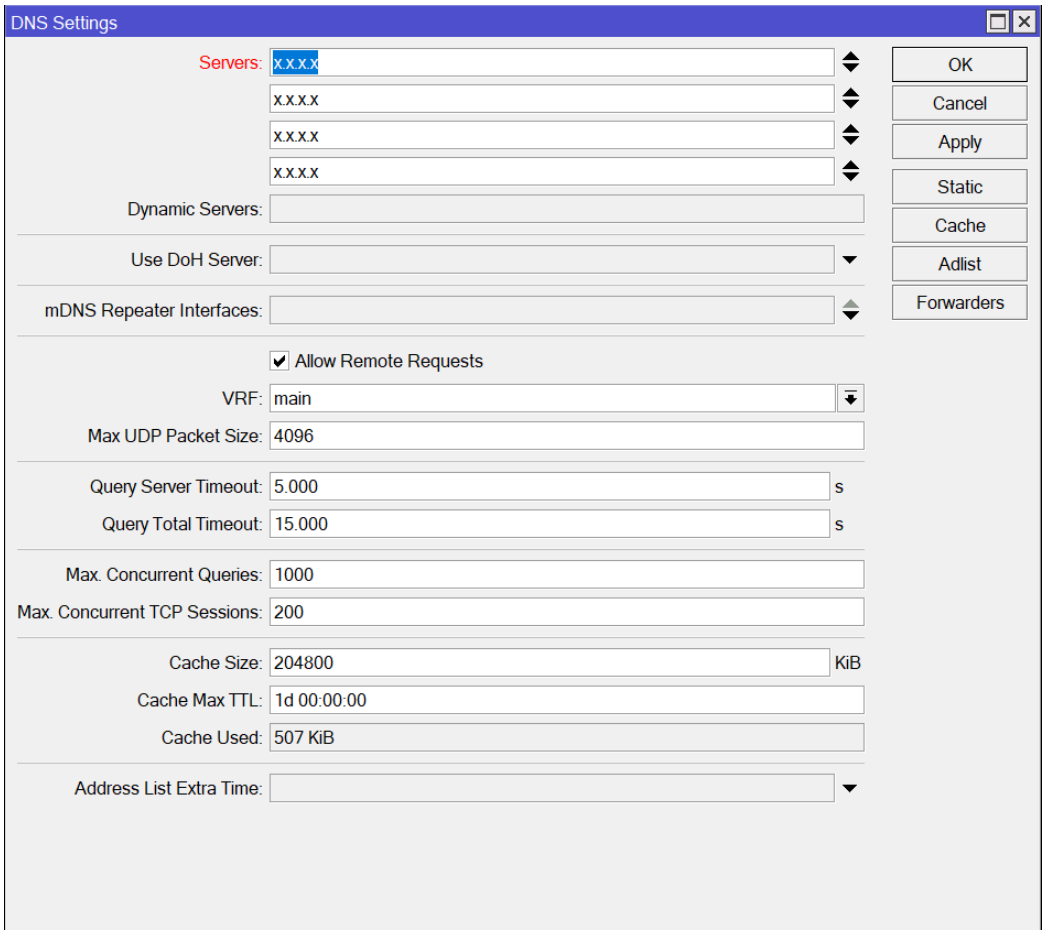

Figura 5. Ejemplo de DNS Settings para un perfil intermedio. Sustituya los servidores por las IP DNS suministradas por IPcom y dimensione según su número de clientes.

Clientes aprox.	cache-size	max-concurrent-queries	max TCP	Observación
Hasta 100	16-32 MiB	200-300	50-100	Routers pequeños/medianos; validar RAM disponible.
101-500	64 MiB	500	100	Punto de partida recomendado para ISP pequeño.
501-1.500	128 MiB	1.000	200	Adecuado para CCR

				con recursos suficientes.
1.501-3.000	256 MiB	2.000	500	Vigilar CPU, cache-used y latencia DNS.
3.001-5.000	512 MiB	3.000	750	Preferible CCR moderno y monitoreo permanente.
Más de 5.000	512 MiB-1 GiB*	4.000+	1.000+	Evaluar resolver dedicado/arquitectura distribuida. *Solo con RAM suficiente.

Parámetros base sugeridos para esta arquitectura: allow-remote-requests=yes; max-udp-packet-size=4096; cache-max-ttl=1d; query-server-timeout=2s; query-total-timeout=10s. Mantenga use-doh-server vacío si el objetivo es reenviar hacia los DNS IPcom configurados en servers. Limite UDP/TCP 53 desde WAN y permita el resolver únicamente a las redes de clientes autorizadas.

```
/ip dns set servers=<DNS_IPCOM_1>,<DNS_IPCOM_2> \
  allow-remote-requests=yes cache-size=128MiB cache-max-ttl=1d \
  max-concurrent-queries=1000 max-concurrent-tcp-sessions=200 \
  max-udp-packet-size=4096 query-server-timeout=2s query-total-timeout=10s
```

> ***Ejemplo mostrado: perfil aproximado para 501-1.500 clientes. No copie los valores de capacidad sin revisar el modelo del router. En equipos con poca RAM, reserve memoria para routing, firewall, colas, BGP/OSPF y demás servicios.***

Monitoreo recomendado después de la puesta en producción: /ip dns print para observar cache-used; /system resource print para RAM/CPU; y contadores del firewall para confirmar que solo las redes autorizadas consultan el resolver. Si cache-used permanece muy por debajo de cache-size, aumentar memoria no aporta beneficio; si la CPU o latencia DNS crecen bajo carga, considere separar la función de resolver.

6.3 NAT: excepciones antes de redirección

Paso A — permitir DNS autorizados

```
/ip firewall nat
add chain=dstnat action=accept protocol=udp in-interface-list=CLIENTES     dst-address-list=DNS-PERMITIDOS
dst-port=53     comment="DNS - Permitir DNS IPcom UDP"

add chain=dstnat action=accept protocol=tcp in-interface-list=CLIENTES     dst-address-list=DNS-PERMITIDOS
dst-port=53     comment="DNS - Permitir DNS IPcom TCP"
```

6.4 NAT: redirección de DNS externo

Paso B — forzar DNS clásico al resolver MikroTik

```
/ip firewall nat
add chain=dstnat action=redirect protocol=udp in-interface-list=CLIENTES     dst-port=53 to-ports=53
comment="DNS - Redireccionar UDP 53"

add chain=dstnat action=redirect protocol=tcp in-interface-list=CLIENTES     dst-port=53 to-ports=53
comment="DNS - Redireccionar TCP 53"
```

> **Por qué UDP y TCP** DNS no utiliza únicamente UDP. TCP/53 es parte normal del protocolo y debe contemplarse para que la política no deje una vía de bypass ni cause fallas ante respuestas que requieran TCP.

6.5 Cómo debe quedar el orden

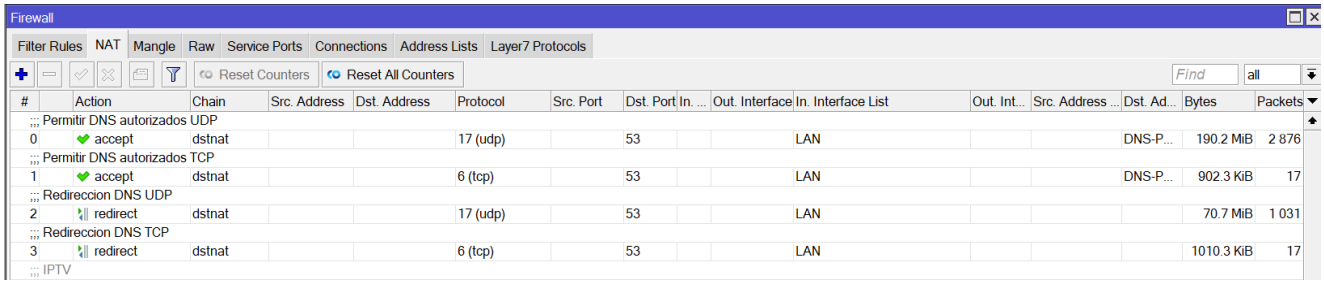

Figura 6. Ejemplo real de NAT: primero se permiten DNS autorizados y luego se redirige UDP/TCP 53 desde LAN.

Orden	Regla	Acción
1	DNS - Permitir DNS IPcom UDP	accept
2	DNS - Permitir DNS IPcom TCP	accept
3	DNS - Redireccionar UDP 53	redirect
4	DNS - Redireccionar TCP 53	redirect

> **Regla de oro** No duplique bloques de NAT. Antes de aplicar una plantilla, busque reglas existentes por comentario y verifique los contadores. Una única política clara es más segura y fácil de auditar que varias copias equivalentes.

6.6 Equivalencia visual en WinBox/WebFig

Las mismas reglas pueden crearse desde IP → Firewall → NAT. La siguiente tabla indica los campos esenciales que deben coincidir.

Regla	General	Action
Permitir UDP	Chain: dstnat · Protocol: udp · In. Interface List: CLIENTES · Dst. Port: 53 · Dst. Address List: DNS-PERMITIDOS	Action: accept
Permitir TCP	Chain: dstnat · Protocol: tcp · In. Interface List: CLIENTES · Dst. Port: 53 · Dst. Address List: DNS-PERMITIDOS	Action: accept
Redirigir UDP	Chain: dstnat · Protocol: udp · In. Interface List: CLIENTES · Dst. Port: 53	Action: redirect · To Ports: 53
Redirigir TCP	Chain: dstnat · Protocol: tcp · In. Interface List: CLIENTES · Dst. Port: 53	Action: redirect · To Ports: 53

7. Control de DNS-over-TLS (DoT)

DNS-over-TLS cifra las consultas DNS y utiliza TCP/853 por defecto. Si la política del ISP exige que los clientes utilicen DNS Seguro de IPcom, permitir DoT externo puede permitir que un equipo evada la redirección de puerto 53.

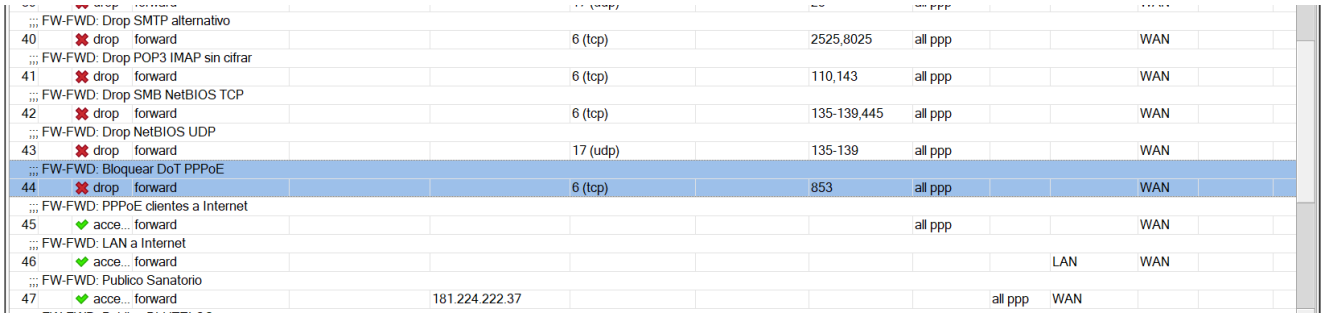

Figura 7. Bloqueo de DoT (TCP/853) ubicado antes de la regla general que permite clientes PPPoE hacia Internet.

Bloqueo DoT para clientes

```
/ip firewall filter
add chain=forward action=drop protocol=tcp in-interface-list=CLIENTES     out-interface-list=WAN dst-port=853
comment="DNS - Bloquear DoT clientes"
```

> **Orden** La regla DoT debe estar antes de la regla general que acepta CLIENTES → WAN. Si queda después, el tráfico ya habrá sido aceptado y el contador de DoT permanecerá en cero.

8. Protección complementaria en RAW y FILTER

8.1 No exponer DNS del router hacia WAN

Protección temprana en RAW

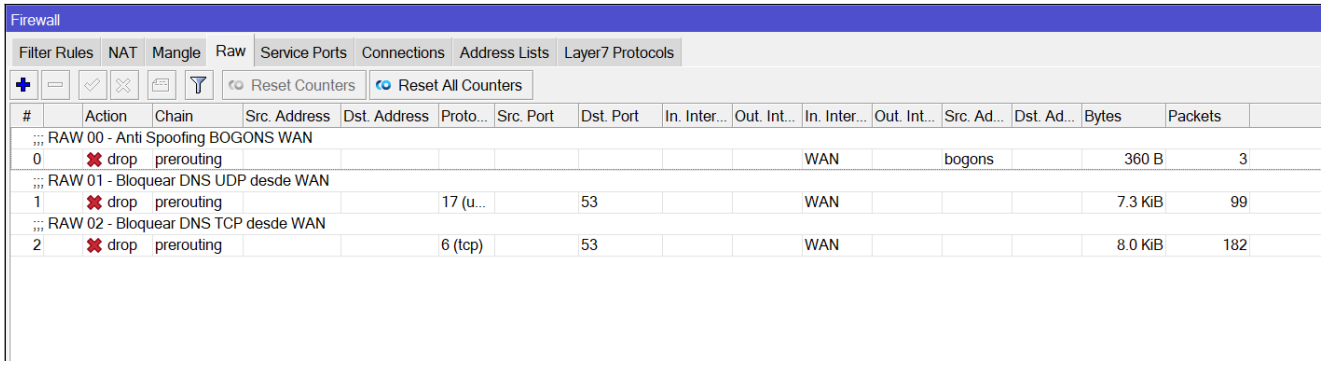

Figura 8. Protección en RAW: anti-spoofing BOGONS y bloqueo de consultas DNS UDP/TCP 53 dirigidas al router desde WAN.

```
/ip firewall raw
add chain=prerouting action=drop protocol=udp in-interface-list=WAN     dst-address-type=local dst-port=53
comment="RAW - Bloquear DNS UDP desde WAN"
add chain=prerouting action=drop protocol=tcp in-interface-list=WAN     dst-address-type=local dst-port=53
comment="RAW - Bloquear DNS TCP desde WAN"
```

Segunda capa en FILTER

```
/ip firewall filter
add chain=input action=drop protocol=udp in-interface-list=WAN dst-port=53     comment="INPUT - Drop DNS
UDP desde WAN"
add chain=input action=drop protocol=tcp in-interface-list=WAN dst-port=53     comment="INPUT - Drop DNS
TCP desde WAN"
```

> **RAW no reemplaza FILTER** RAW es útil para descartar tráfico antes de connection tracking, pero no debe convertirse en una copia completa del firewall stateful. Mantenga las decisiones dependientes de estado en FILTER.

8.2 Anti-spoofing con bogons

Una regla RAW de anti-spoofing puede ser útil si el ISP mantiene una lista BOGONS correcta y compatible con su upstream. No copie listas genéricas sin revisar el direccionamiento de tránsito: algunos operadores utilizan RFC1918 o CGNAT en enlaces WAN.

Ejemplo opcional de anti-spoofing

```
/ip firewall raw
add chain=prerouting action=drop in-interface-list=WAN     src-address-list=BOGONS comment="RAW - Anti
Spoofing BOGONS WAN"
```

9. ICMP, PMTU y PPPoE

Una redirección DNS puede parecer defectuosa cuando el problema real es MTU/PMTU. En redes PPPoE es especialmente importante no bloquear ICMP de forma indiscriminada. ICMP Destination Unreachable / Fragmentation Required (tipo 3, código 4) participa en Path MTU Discovery para IPv4.

ICMP IPv4	Uso
0:0 Echo Reply	Diagnóstico
3:0 Network Unreachable	Errores de alcance
3:1 Host Unreachable	Errores de alcance
3:4 Fragmentation Required	PMTU — crítico en escenarios PPPoE
8:0 Echo Request	Diagnóstico
11:0 Time Exceeded	Traceroute / TTL
12:0 Parameter Problem	Diagnóstico de cabecera

IPv6 No replique una política restrictiva de ICMPv4 sobre ICMPv6 sin diseño específico. IPv6 depende de ICMPv6 para funciones esenciales como Neighbor Discovery y Packet Too Big.

10. Consideraciones sobre DoH

DNS-over-HTTPS (DoH) utiliza HTTPS y normalmente comparte TCP/443 con navegación web. Por ello no existe una regla simple equivalente a “bloquear puerto 853” que sea segura para todos los entornos. Bloquear 443 indiscriminadamente rompería servicios legítimos.

- Trate DoH como una política separada de la redirección DNS clásica.
- En redes gestionadas, prefiera políticas de endpoint/navegador o listas mantenidas de resolvers DoH cuando sea apropiado.
- Considere HTTP/3/QUIC (UDP/443) antes de concluir que bloquear TCP/443 controla DoH.
- Valide siempre el impacto antes de aplicar bloqueos a servicios cifrados compartidos.

11. Validación y pruebas

11.1 Verificar configuración

Comandos de auditoría

```
/ip dns print
/ip firewall address-list print detail where list="DNS-PERMITIDOS"
/ip firewall nat print detail where comment~"DNS"
/ip firewall filter print detail where comment~"DoT|DNS"
/ip firewall raw print detail where comment~"DNS|BOGON"
```

11.2 Verificar contadores

Contadores de tráfico

```
/ip firewall nat print stats without-paging
/ip firewall filter print stats without-paging
/ip firewall raw print stats without-paging
```

Prueba	Resultado esperado
Cliente configurado con DNS IPcom	La regla “Permitir DNS IPcom” incrementa contadores; no hay redirect
Cliente configurado con 8.8.8.8 o 1.1.1.1	El redirect UDP/TCP 53 incrementa contadores y el nombre sigue resolviendo
Intento DoT a un resolver externo	La regla TCP/853 incrementa contadores y la sesión no se establece
Consulta DNS desde Internet hacia el MikroTik	RAW/FILTER WAN 53 descartan el intento
Ping / PMTU	No aparecen fallas causadas por bloqueo excesivo de ICMP

> **Prueba práctica** Después de cambiar una regla NAT, recuerde que NAT actúa sobre el primer paquete de una conexión. Para pruebas controladas puede ser necesario esperar a que expire la conexión previa o limpiar únicamente las conexiones de laboratorio pertinentes.

12. Diagnóstico y resolución de problemas

Síntoma	Causa probable	Qué revisar
No navega después del redirect	Resolver local no responde / INPUT bloquea clientes	/ip dns, allow-remote-requests, reglas INPUT 53
DNS externo sigue funcionando sin contadores	Regla no alcanza al cliente o está después de otra coincidencia	Interface-list, src-address, orden NAT
DNS IPcom también se redirige	Excepciones DNS-PERMITIDOS faltantes o después del redirect	Orden 1–4
DoT sigue conectando	Drop 853 está después del accept general	Orden en forward
Algunas webs cargan lento	PMTU/MTU, pérdida, radio o upstream; no asumir DNS	ICMP 3:4, ping DF, latencia
Router visible como DNS desde Internet	Falta protección WAN	RAW/FILTER input UDP/TCP 53

13. Checklist de puesta en producción

- ☐ Backup/export realizado antes del cambio.
- ☐ WAN y LAN están separadas en interface lists.
- ☐ Existe una selección explícita de interfaces/redes CLIENTES.
- ☐ DNS-PERMITIDOS contiene únicamente los resolvers autorizados por IPcom.
- ☐ El MikroTik utiliza DNS Seguro IPcom como upstream.
- ☐ DNS Settings fue dimensionado según clientes, hardware y concurrencia real.

- ☐ allow-remote-requests está limitado por firewall a redes autorizadas.
- ☐ Excepciones UDP/TCP 53 están antes de las reglas redirect.
- ☐ Redirect UDP 53 y TCP 53 está activo para CLIENTES.
- ☐ Drop DoT TCP/853 está antes del accept general hacia WAN.
- ☐ DNS desde WAN al router está bloqueado en RAW/FILTER.
- ☐ ICMP/PMTU fue revisado, especialmente en PPPoE.
- ☐ Contadores NAT/FILTER/RAW fueron verificados después del cambio.
- ☐ Se probó un DNS permitido, uno externo y un intento DoT.

☐ Se validó la política de bloqueo MinTIC/autoridades y la página de bloqueo esperada.

☐ Se documentaron excepciones propias del ISP.

14. Reversión segura

Si durante la implementación aparece un comportamiento inesperado, deshabilite primero las reglas nuevas en lugar de borrarlas. Esto conserva el orden, los comentarios y la posibilidad de comparar contadores.

Ejemplo de reversión temporal

```
/ip firewall nat disable [find where comment~"DNS - Redireccionar"]
/ip firewall filter disable [find where comment="DNS - Bloquear DoT clientes"]
```

> **Evite cambios masivos** No elimine reglas de producción por número si la tabla puede cambiar de orden. Use comentarios únicos para localizar las reglas y verifique el resultado antes de continuar.

15. Referencias técnicas

MikroTik RouterOS — DNS — Documenta allow-remote-requests, cache-size, cache-max-ttl, max-concurrent-queries, max-concurrent-tcp-sessions y timeouts del resolver.
https://help.mikrotik.com/docs/spaces/ROS/pages/37748767/DNS

MikroTik RouterOS — NAT — La acción redirect cambia el destino hacia la dirección de la interfaz de entrada y permite especificar to-ports.
https://help.mikrotik.com/docs/spaces/ROS/pages/3211299/NAT

MikroTik RouterOS — Firewall — Describe cadenas, orden de evaluación y funciones de NAT/FILTER/RAW.
https://help.mikrotik.com/docs/spaces/ROS/pages/250708066/Firewall

MikroTik RouterOS — RAW Filtering — RAW puede procesar tráfico antes de connection tracking y dispone de prerouting/output.
https://help.mikrotik.com/docs/spaces/ROS/pages/48660574/Filter

MikroTik RouterOS — Interface Lists — Las listas permiten agrupar interfaces y simplificar configuraciones de firewall.
https://help.mikrotik.com/docs/spaces/ROS/pages/47579180/Interface+Lists

RFC 7858 — DNS over TLS — Define TCP/853 como puerto por defecto para DoT.
https://www.rfc-editor.org/rfc/rfc7858

IPcom Sistemas S.A.S. - DNS + Firewall / Bloqueos ISP - Describe la protección DNS, listados MinTIC, Coljuegos, abuso infantil, Magis TV, órdenes judiciales, reputación IP y actualización centralizada de zonas.
https://bloqueos-isp-mintic.com/dns/
https://bloqueos-isp-mintic.com/

Documento vivo Las topologías ISP cambian. Antes de reutilizar esta plantilla en otro router, confirme interfaces, pools, VPN, routing, reglas existentes y direcciones DNS autorizadas. La seguridad depende tanto de la regla como de su contexto.

IPcom Sistemas S.A.S. · DNS Seguro

Control del documento

Versión	Fecha	Audiencia	Estado
1.1	Agosto 2026	ISP clientes de DNS Seguro IPcom	Guía de referencia

Antes de reutilizar esta guía

- Reemplace <DNS_IPCOM_1> y <DNS_IPCOM_2> por los resolvers asignados.
- Reemplace <INTERFAZ_WAN> y <INTERFAZ_LAN> por su topología real.
- Confirme que VPN, OSPF/BGP, administración, WispHub u otros servicios no queden dentro de la política CLIENTES por error.
- Pruebe primero con un grupo controlado y valide contadores antes de ampliar la política.