PROZCENTER
CENTRO DE PROFESIONALES

Seguridad y BGP en RouterOS v7

Mayo 2024, CABA

CÁMARA ARGENTINA DE Internet

XX Encuentro Nacional de Técnicos

Objetivos de esta presentación

- **Implementación de BGP en RouterOS v7**:
  - Filtros
  - Publicación de redes
  - Configuración de peers

- **Repaso de cuestiones relacionadas con ciberseguridad**:
  - Servicios capa 2
  - Servicios capa 3
  - Firewall
  - Accesos VPN

BGP en RouterOS v7

XX Encuentro Nacional de Técnicos

Diferencias entre RouterOS v6 y v7

- BGP (y todo el sistema de ruteo) fue reescrito por completo.
- Las secciones instance y peer se reemplazan con connection y session.
- También existe una sección template para no tener que repetir datos en cada connection.
- La sección network se reemplaza con address-list (dentro de /ip firewall)
- Los filtros fueron totalmente reemplazados, ahora se escriben con una notación tipo código.

Implementación BGP de RouterOS v7

- Una forma ordenada de configurar BGP en v7 sería la siguiente:

1) **Configurar filtros** (lo mas dificil primero)
   En /routing filter
2) **Configurar distribución de redes** (se hace de una manera exótica)
   En /routing bgp connection y en /ip firewall address-list
3) **Levantar peers** (fácil)
   En /routing bgp connection, parámetros mínimos (v7.14.3):
   name, as, remote.address, remote.as, local.role.

Routing Filters en BGP de RouterOS v7

Routing Filters en BGP de RouterOS v7

- En ROSv7 los filtros BGP fueron implementados con una sintaxis tipo script o código.
- Cada regla puede contener múltiples condiciones y acciones:

```
if (condiciones) {acciones} else {acciones}
```

- Recomiendo usar Notepad++ con lenguaje C# para escribir los filtros y luego pasarlos al router. Si bien no corrige sintaxis BGP, al menos nos va a permitir evitar errores de tipeo.
- Referencia de condiciones y acciones: https://help.mikrotik.com/docs/display/ROS/Route+Selection+and+Filters

Routing Filters en BGP de RouterOS v7

- Crear una cadena (conjunto) de reglas para filtrar rutas

  /routing filter rule add chain=filter1_out

- Este comando crea una cadena vacía sin reglas, y que en ROSv7 por defecto descarta todo (action=discard, las rutas permanecen en memoria pero no pasan a la FIB).

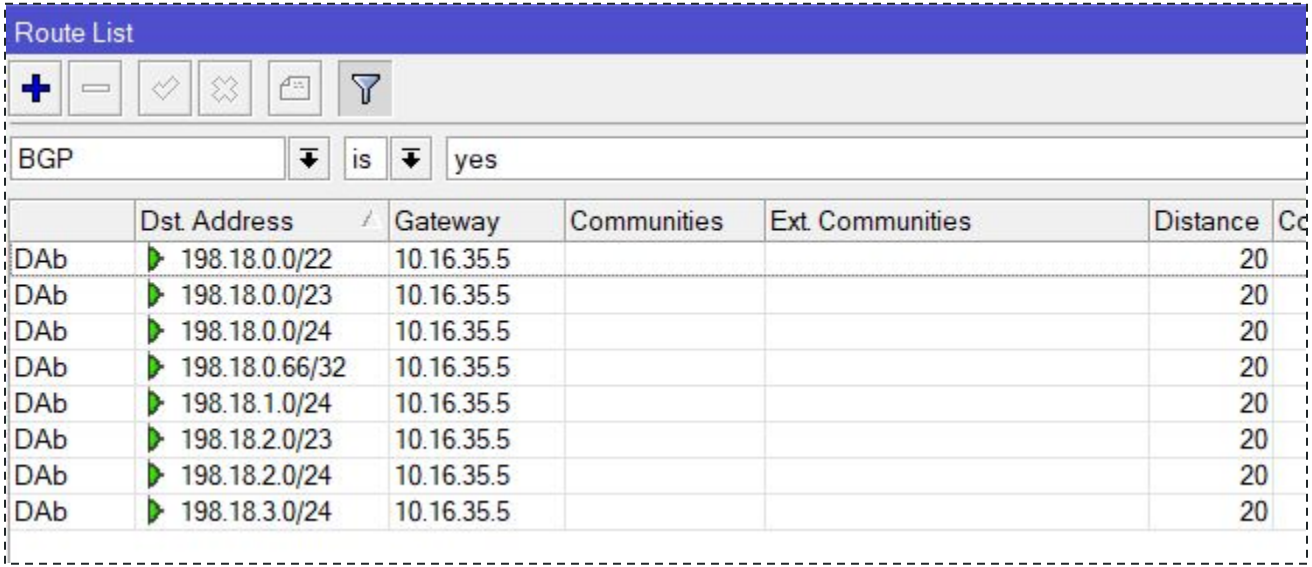
Routing Filters en BGP de RouterOS v7

- Ejemplo para permitir prefijos propios (suponiendo que tengo asignado un prefijo 198.18.0.0/22):
  a. Condición: destino=198.18.0.0/22, Acción: aceptar
  b. if (dst in 198.18.0.0/22) {accept}

- /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22) {accept}"

Routing Filters en BGP de RouterOS v7

- El resultado real, dependerá de cómo se han publicado prefijos dentro del /22 definido en el filtro.



	Dst. Address	Gateway	Communities	Ext. Communities	Distance	Cc
DAb	198.18.0.0/22	10.16.35.5			20	
DAb	198.18.0.0/23	10.16.35.5			20	
DAb	198.18.0.0/24	10.16.35.5			20	
DAb	198.18.0.66/32	10.16.35.5			20	
DAb	198.18.1.0/24	10.16.35.5			20	
DAb	198.18.2.0/23	10.16.35.5			20	
DAb	198.18.2.0/24	10.16.35.5			20	
DAb	198.18.3.0/24	10.16.35.5			20	

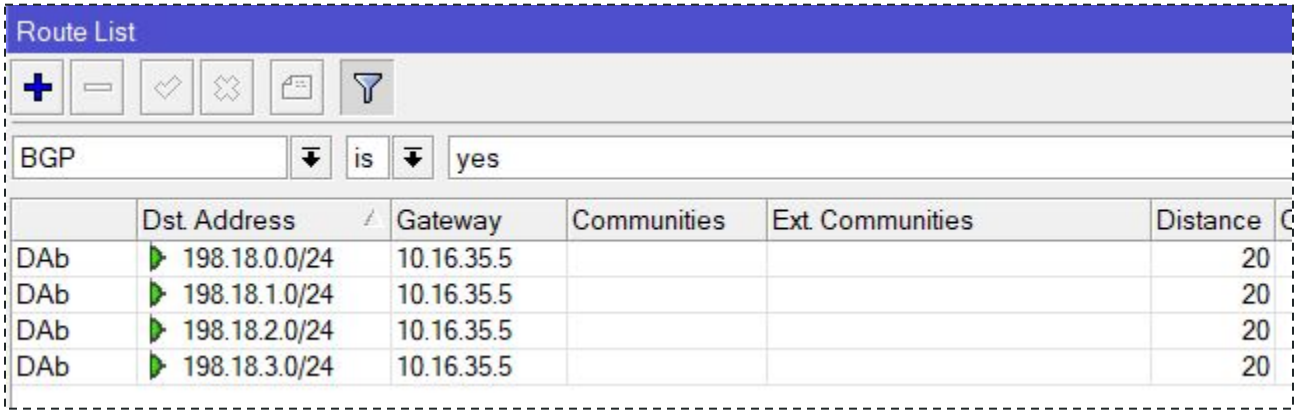
Routing Filters en BGP de RouterOS v7

- Si quiero publicar el /22, pero dividido en /24, debo agregar más condiciones:
  a. Condición: destino=198.18.0.0/22, prefijo=24, Acción: aceptar
  b. if (dst in 198.18.0.0/22 && dst-len==24) {accept}

- /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22 && dst-len==24) {accept}"

Routing Filters en BGP de RouterOS v7

- Agregando más condiciones, puedo publicar prefijos de manera más precisa y evitar route leaks (fuga de rutas).



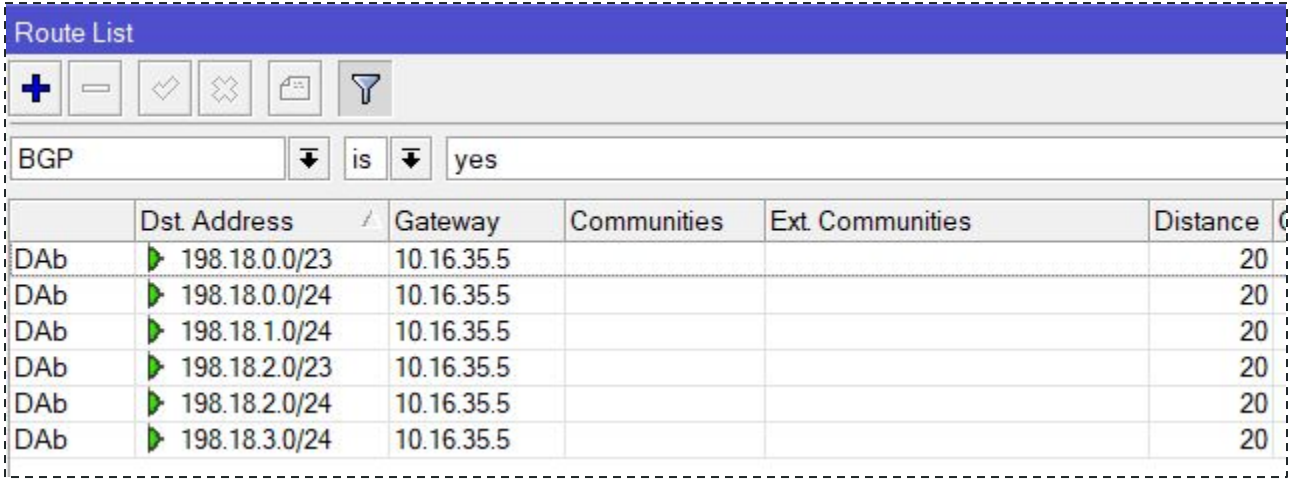
Routing Filters en BGP de RouterOS v7

- Si quiero publicar el /22, pero dividido en /24 0 /23, debo agregar otra condición extra:
  a. Condición: destino=198.18.0.0/22, prefijo=24 o 23, Acción: aceptar
  b. if (dst in 198.18.0.0/22 && dst-len in 23-24) {accept}

- /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22 && dst-len in 23-24) {accept}"

Routing Filters en BGP de RouterOS v7

- Agregando más condiciones, puedo publicar prefijos de manera más precisa y evitar route leaks (fuga de rutas).



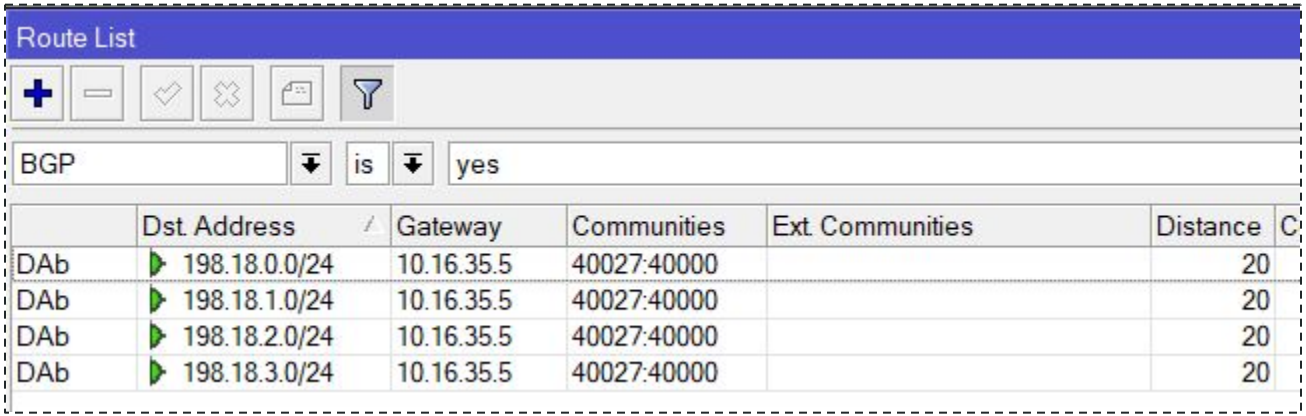
Routing Filters en BGP de RouterOS v7

- Para agregar comunidades, deberíamos agregar una acción adicional:

- ```
  /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22 && dst-len==24) \
  {set bgp-communities 40027:40000; accept}"
  ```
  ```

Routing Filters en BGP de RouterOS v7

- Agregando más acciones, puedo publicar prefijos con comunidades simples:



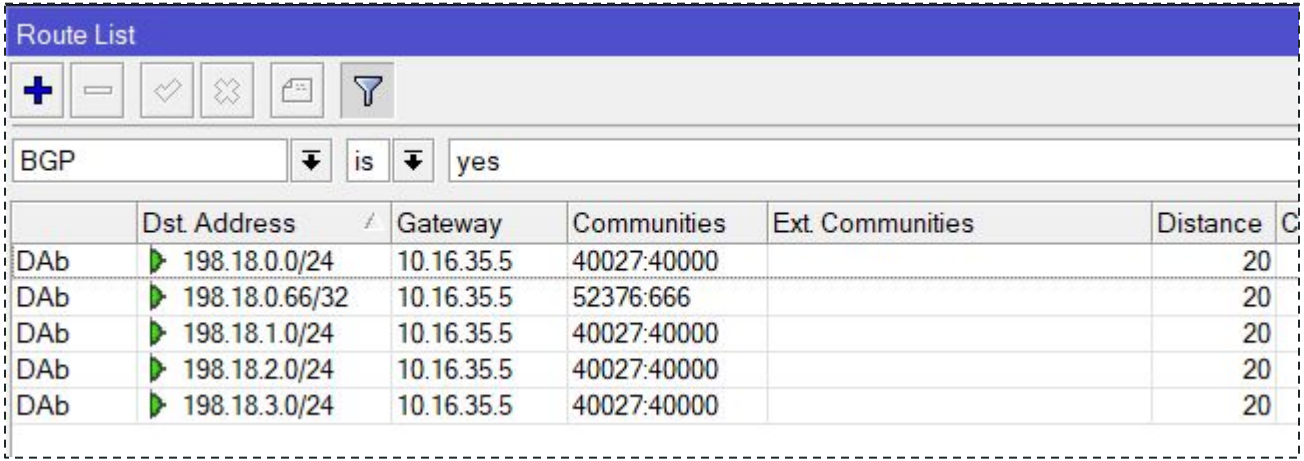
Routing Filters en BGP de RouterOS v7

- Para agregar comunidades simples, como la de blackhole utilizada en varios IXPs/Carriers.

- ```
  /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst==198.18.0.66/32) \
  {set bgp-communities 52376:666; accept}"
  ```
  ```

Routing Filters en BGP de RouterOS v7

- Agregando más acciones, puedo publicar prefijos con comunidades simples:



	Dst. Address	Gateway	Communities	Ext. Communities	Distance	C
DAb	198.18.0.0/24	10.16.35.5	40027:40000		20	
DAb	198.18.0.66/32	10.16.35.5	52376:666		20	
DAb	198.18.1.0/24	10.16.35.5	40027:40000		20	
DAb	198.18.2.0/24	10.16.35.5	40027:40000		20	
DAb	198.18.3.0/24	10.16.35.5	40027:40000		20	

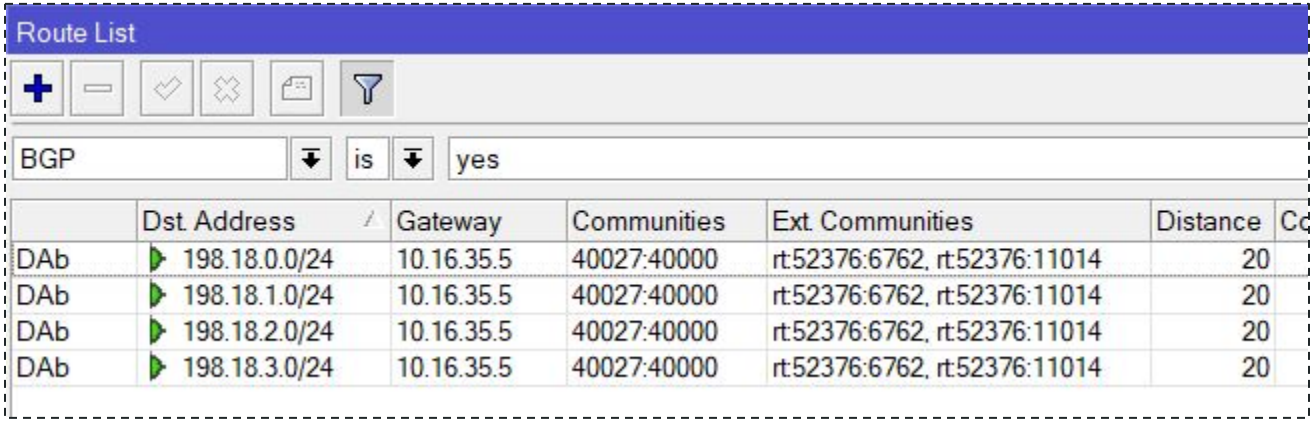
Routing Filters en BGP de RouterOS v7

- Para agregar comunidades extendidas, deberíamos agregar otra acción adicional:

- ```
  /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22 && dst-len==24) \
  {set bgp-communities 40027:40000; \
  append bgp-ext-communities rt:52376:11014,rt:52376:6762; \
  accept}"
  ```
  ```

Routing Filters en BGP de RouterOS v7

- Agregando más acciones, puedo publicar prefijos con comunidades extendidas:



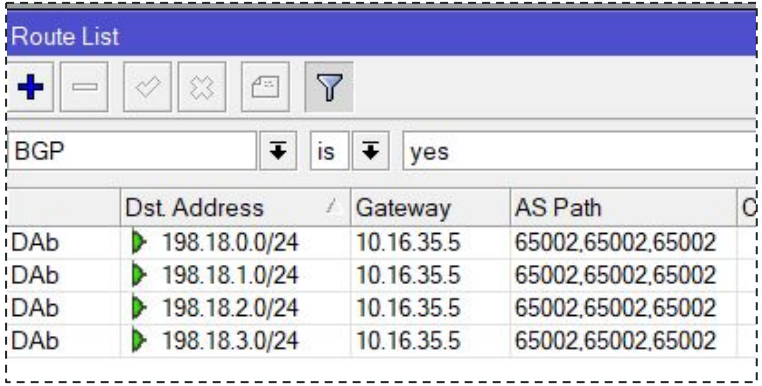
	Dst. Address	Gateway	Communities	Ext. Communities	Distance	Cc
DAb	198.18.0.0/24	10.16.35.5	40027:40000	rt:52376:6762, rt:52376:11014	20	
DAb	198.18.1.0/24	10.16.35.5	40027:40000	rt:52376:6762, rt:52376:11014	20	
DAb	198.18.2.0/24	10.16.35.5	40027:40000	rt:52376:6762, rt:52376:11014	20	
DAb	198.18.3.0/24	10.16.35.5	40027:40000	rt:52376:6762, rt:52376:11014	20	

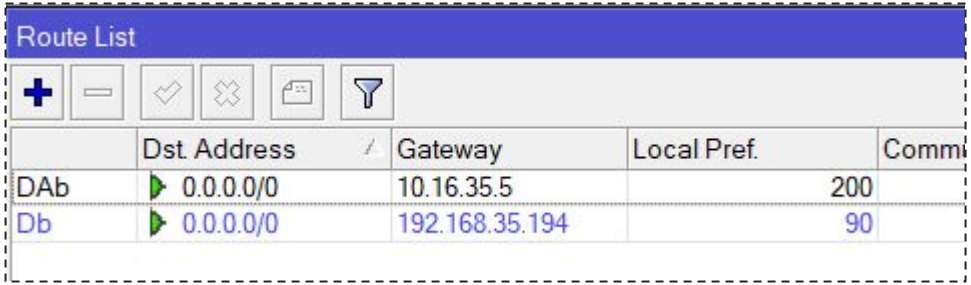
Routing Filters en BGP de RouterOS v7

- Para agregar bgp-path-prepend o local-pref, usamos acciones adicionales:
- /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 198.18.0.0/22 && dst-len==24) \
  {set bgp-path-prepend 3; accept}"
- /routing filter rule add chain=filter1_out disabled=no \
  rule="if (dst in 0.0.0.0/0 && dst-len==0) \
  {set bgp-local-pref 200; accept}"

Routing Filters en BGP de RouterOS v7

- Agregando más acciones, puedo publicar prefijos con comunidades extendidas:





Distribución de redes IPv4/IPv6

Distribución de redes IPv4/IPv6

- En ROSv6 desde /routing bgp network se hacía la distribución de prefijos. Se podían cargar redes sincronizadas con la tabla de ruteo (ej sync=yes) o cualquier red (ej network=8.8.0.0/16 sync=no).
- En ROSv7 sólo pueden publicarse prefijos con un address-list del firewall de IPv4/IPv6, pero esos prefijos deben existir en la tabla de ruteo.
- En caso de que esto no sea posible, debe crearse una ruta blackhole.

Distribución de redes IPv4/IPv6

- Para publicar prefijos /24 del 198.18.0.0/22, hay que:

```
/ip firewall address-list
add address=198.18.0.0/24 list=alist_bgp_networks-ip4
add address=198.18.1.0/24 list=alist_bgp_networks-ip4
add address=198.18.2.0/24 list=alist_bgp_networks-ip4
add address=198.18.3.0/24 list=alist_bgp_networks-ip4

/ip route
add address=198.18.0.0/24 disabled=no blackhole
add address=198.18.1.0/24 disabled=no blackhole
add address=198.18.2.0/24 disabled=no blackhole
add address=198.18.3.0/24 disabled=no blackhole
```

Distribución de redes IPv4/IPv6

- Una alternativa para publicar prefijos /24 del 198.18.0.0/22:

```
/routing bgp connection
set [find name=peerx] output.redistribute=static

/ip route
add address=198.18.0.0/24 disabled=no blackhole
add address=198.18.1.0/24 disabled=no blackhole
add address=198.18.2.0/24 disabled=no blackhole
add address=198.18.3.0/24 disabled=no blackhole
```

Configuración de peers BGP

Parámetros para configurar un peer BGP

- **Mínimos**:
  - name, as, local.role
  - remote.as, remote.address
- **Deseables**:
  - address-families
  - input.filter, output.filter-chain
  - output.network, output.redistribute

Ejemplo de conexión IPv4 + IPv6 con IXP (CABASE)

```
/routing bgp connection
add name=cabase \
1 as=123456 local.role=ebgp disabled=no \
  remote.as=52376 remote.address=45.68.8.254 \
2 input.filter=cabase_in output.filter-chain=cabase_out \
3 address-families=ip \
  output.network=alist_bgp_networks-ip4
```

```
/routing bgp connection
add name=cabasev6 as=123456 \
1 remote.as=52376 remote.address=2001:13c7:6001::8:254 \
  local.role=ebgp disabled=no \
2 input.filter=cabasev6_in output.filter-chain=cabasev6_out \
3 address-families=ipv6 \
  output.network=alist_bgp_networks-ip6
```

Ejemplo de conexión con TIP IPv4 + IPv6

```
/routing bgp connection
1 add name=tipx as=123456 \
  remote.as=7890 remote.address=192.0.2.1 \
  local.role=ebgp disabled=no \
2 input.filter=tipx_in output.filter-chain=tipx_out \
3 address-families=ip,ipv6 \
  output.redistribute=static
```

Para poder definir qué publicar, debo manejarme con rutas blackhole (IPv4/IPv6) y los filtros (mucho cuidado!)

Ejemplo de conexión multihop IPv4 + IPv6 (UTRS)

```
/routing bgp connection
add name=teamcymru-utrs as=123456  local.address=198.51.100.1 \
1
remote.as=64496 remote.address=216.31.8.100/32 \
connect=no listen=yes multihop=yes local.role=ebgp disabled=no \
2
input.filter=teamcymru-utrs_in output.filter-chain=teamcymru-utrs_out \
address-families=ip,ipv6 \
3
output.network=alist_bgp_networks-ip4-utrs

output.redistribute=static
```

Para poder definir qué publicar, debo manejarme con rutas blackhole (IPv4/IPv6) y los filtros (mucho cuidado!)

Ejemplo de conexión iBGP

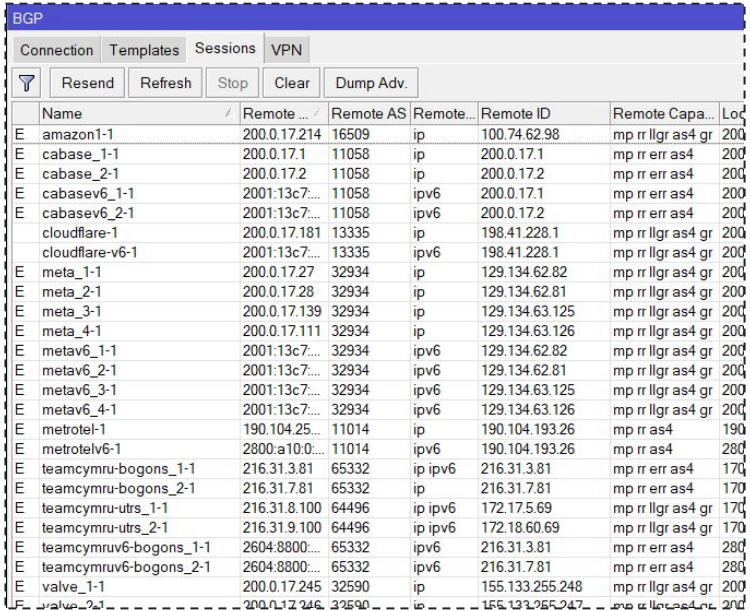
```
/routing bgp connection
add name=router1 as=123456  local.address=10.255.0.1 \
remote.as=123456 remote.address=10.255.0.2 \
local.role=ibgp-rr disabled=no \
input.filter=ibgp_in output.filter-chain=ibgp_out \
address-families=ip,ipv6 \

/routing bgp connection
add name=router2 as=123456  local.address=10.255.0.2 \
remote.as=123456 remote.address=10.255.0.1 \
local.role=ibgp-rr-client disabled=no \
input.filter=ibgp_in output.filter-chain=ibgp_out \
address-families=ip,ipv6 \
```

1
2
3

Estado de los peers

- En ROSv7, el estado del peer se ve en /routing bgp session print



	Name	Remote ...	Remote AS	Remote...	Remote ID	Remote Capa...	Lo
E	amazon1-1	200.0.17.214	16509	ip	100.74.62.98	mp rr llgr as4 gr	200
E	cabase_1-1	200.0.17.1	11058	ip	200.0.17.1	mp rr err as4	200
E	cabase_2-1	200.0.17.2	11058	ip	200.0.17.2	mp rr err as4	200
E	cabasev6_1-1	2001:13c7:...	11058	ipv6	200.0.17.1	mp rr err as4	200
E	cabasev6_2-1	2001:13c7:...	11058	ipv6	200.0.17.2	mp rr err as4	200
	cloudflare-1	200.0.17.181	13335	ip	198.41.228.1	mp rr llgr as4 gr	200
	cloudflare-v6-1	2001:13c7:...	13335	ipv6	198.41.228.1	mp rr llgr as4 gr	200
E	meta_1-1	200.0.17.27	32934	ip	129.134.62.82	mp rr llgr as4 gr	200
E	meta_2-1	200.0.17.28	32934	ip	129.134.62.81	mp rr llgr as4 gr	200
E	meta_3-1	200.0.17.139	32934	ip	129.134.63.125	mp rr llgr as4 gr	200
E	meta_4-1	200.0.17.111	32934	ip	129.134.63.126	mp rr llgr as4 gr	200
E	metav6_1-1	2001:13c7:...	32934	ipv6	129.134.62.82	mp rr llgr as4 gr	200
E	metav6_2-1	2001:13c7:...	32934	ipv6	129.134.62.81	mp rr llgr as4 gr	200
E	metav6_3-1	2001:13c7:...	32934	ipv6	129.134.63.125	mp rr llgr as4 gr	200
E	metav6_4-1	2001:13c7:...	32934	ipv6	129.134.63.126	mp rr llgr as4 gr	200
E	metrotel-1	190.104.25...	11014	ip	190.104.193.26	mp rr as4	190
E	metrotelv6-1	2800:a10:0:...	11014	ipv6	190.104.193.26	mp rr as4	280
E	teamcymru-bogons_1-1	216.31.3.81	65332	ip ipv6	216.31.3.81	mp rr err as4	170
E	teamcymru-bogons_2-1	216.31.7.81	65332	ip	216.31.7.81	mp rr err as4	170
E	teamcymru-utrs_1-1	216.31.8.100	64496	ip ipv6	172.17.5.69	mp rr llgr as4 gr	170
E	teamcymru-utrs_2-1	216.31.9.100	64496	ip ipv6	172.18.60.69	mp rr llgr as4 gr	170
E	teamcymruv6-bogons_1-1	2604:8800:...	65332	ipv6	216.31.3.81	mp rr err as4	280
E	teamcymruv6-bogons_2-1	2604:8800:...	65332	ipv6	216.31.7.81	mp rr err as4	280
E	valve_1-1	200.0.17.245	32590	ip	155.133.255.248	mp rr llgr as4 gr	200
E	valve_2-1	200.0.17.246	32590	ip	155.133.255.247	mp rr llgr as4 gr	200

```
Flags: E - established
 0 E name="metrotel-1"
     remote.address=190.104.253.44 .as=11014 .id=190.104.193.26
     .capabilities=mp,rr,as4 .messages=41900 .bytes=796129 .eor=ip
     local.address=[redacted] .as=[redacted] .id=[redacted]
     .capabilities=mp,rr,gr,as4 .messages=41900 .bytes=796137 .eor=""
     output.procid=20 .filter-chain=metrotel_out
     .network=alist_bgp_networks-ip4
     input.procid=20 .filter=metrotel_in ebgp
     hold-time=3m keepalive-time=1m uptime=4w1d2h19m48s350ms
     last-started=2024-04-15 18:26:12 prefix-count=1

 1 E name="cabase_2-1"
     remote.address=200.0.17.2 .as=11058 .id=200.0.17.2
     .capabilities=mp,rr,as4,err .hold-time=1m30s .messages=339917
     .bytes=49405186 .eor=ip
     local.address=[redacted] .as=[redacted] .id=[redacted]
     .capabilities=mp,rr,gr,as4 .messages=83797 .bytes=1592318 .eor=""
     output.procid=21 .filter-chain=cabase_out
     .network=alist_bgp_networks-ip4
     input.procid=21 .filter=cabase_in ebgp
     hold-time=1m30s keepalive-time=30s uptime=4w1d2h19m38s830ms
     last-started=2024-04-15 18:26:22 prefix-count=26683
-- [Q quit|down]
```

Monitoreo BGP

Ver prefijos publicados

- En ROSv7, los prefijos publicados se pueden ver en /routing bgp advertisements print

```
[admin@R1] > routing/bgp/advertisements/print
 0 peer=bgp1-1 dst=198.18.0.0/24 afi=ip nexthop=169.254.1.1 origin=0 as-path=sequence 65001

 0 peer=bgp1-1 dst=198.18.1.0/24 afi=ip nexthop=169.254.1.1 origin=0 as-path=sequence 65001

 0 peer=bgp1-1 dst=198.18.2.0/24 afi=ip nexthop=169.254.1.1 origin=0 as-path=sequence 65001

 0 peer=bgp1-1 dst=198.18.3.0/24 afi=ip nexthop=169.254.1.1 origin=0 as-path=sequence 65001

 0 peer=bgp1-1 dst=198.18.0.66 afi=ip nexthop=169.254.1.1 origin=0 as-path=sequence 65001 communities=52376:666

 0 peer=bgp1-1 dst=2001:db8:acdc::/48 afi=ipv6 nexthop=::ffff:169.254.1.1 origin=0 as-path=sequence 65001
[admin@R1] >
```

Ver prefijos recibidos

- En ROSv7, los prefijos recibidos se pueden ver en /routing route print where **belongs-to**~"169.254.1.1"

```
[admin@R2] > routing/route/print where belongs-to~"169.254.1.1"
Flags: U - UNREACHABLE, A - ACTIVE; b - BGP; H - HW-OFFLOADED
Columns: DST-ADDRESS, GATEWAY, AFI, DISTANCE, SCOPE, TARGET-SCOPE, IMMEDIATE-GW
    DST-ADDRESS         GATEWAY              AFI  DISTANCE  SCOPE  TARGET-SCOPE  IMMEDIATE-GW
Ab  198.18.0.0/24       169.254.1.1          ip4        20     40            10  169.254.1.1%ether1
Ab  198.18.0.66/32      169.254.1.1          ip4        20     40            10  169.254.1.1%ether1
Ab  198.18.1.0/24       169.254.1.1          ip4        20     40            10  169.254.1.1%ether1
Ab  198.18.2.0/24       169.254.1.1          ip4        20     40            10  169.254.1.1%ether1
Ab  198.18.3.0/24       169.254.1.1          ip4        20     40            10  169.254.1.1%ether1
UbH 2001:db8:acdc::/48  ::ffff:169.254.1.1.1 ip6        20     40            10
[admin@R2] >
```

Seguridad en RouterOS v7

CÁMARA ARGENTINA DE Internet

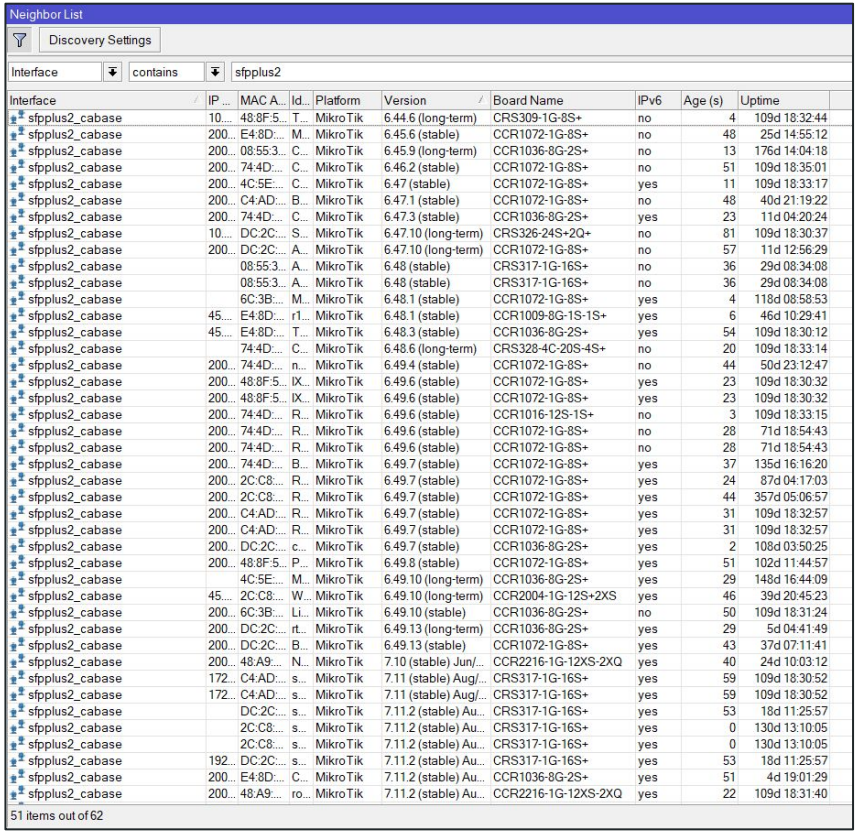
XX Encuentro Nacional de Técnicos

Mecanismos de seguridad

Módulos para aplicar mecanismos de Seguridad

- **Servicios capa 2** ➡️ /ip neighbor discovery-settings
  ➡️ /tool romon
- **Servicios capa 3** ➡️ /ip service
- **Firewall** ➡️ /ip firewall
- **Accesos VPN** ➡️ /ppp
  ➡️ /interface wireguard

MNDP - MikroTik Neighbor Discovery protocol



Interface	IP ...	MAC A...	Id...	Platform	Version	Board Name	IPv6	Age (s)	Uptime
sfpplus2_cabase	10....	48:8F:5...	T...	MikroTik	6.44.6 (long-term)	CRS309-1G-8S+	no	4	109d 18:32:44
sfpplus2_cabase	200...	E4:8D:...	M...	MikroTik	6.45.6 (stable)	CCR1072-1G-8S+	no	48	25d 14:55:12
sfpplus2_cabase	200...	08:55:3...	C...	MikroTik	6.45.9 (long-term)	CCR1036-8G-2S+	no	13	176d 14:04:18
sfpplus2_cabase	200...	74:4D:...	C...	MikroTik	6.46.2 (stable)	CCR1072-1G-8S+	no	51	109d 18:35:01
sfpplus2_cabase	200...	4C:5E:...	C...	MikroTik	6.47 (stable)	CCR1072-1G-8S+	yes	11	109d 18:33:17
sfpplus2_cabase	200...	C4:AD:...	B...	MikroTik	6.47.1 (stable)	CCR1072-1G-8S+	no	48	40d 21:19:22
sfpplus2_cabase	200...	74:4D:...	C...	MikroTik	6.47.3 (stable)	CCR1036-8G-2S+	yes	23	11d 04:20:24
sfpplus2_cabase	10....	DC:2C:...	S...	MikroTik	6.47.10 (long-term)	CRS326-24S+2Q+	no	81	109d 18:30:37
sfpplus2_cabase	200...	DC:2C:...	A...	MikroTik	6.47.10 (long-term)	CCR1072-1G-8S+	no	57	11d 12:56:29
sfpplus2_cabase		08:55:3...	A...	MikroTik	6.48 (stable)	CRS317-1G-16S+	no	36	29d 08:34:08
sfpplus2_cabase		08:55:3...	A...	MikroTik	6.48 (stable)	CRS317-1G-16S+	no	36	29d 08:34:08
sfpplus2_cabase		6C:3B:...	M...	MikroTik	6.48.1 (stable)	CCR1072-1G-8S+	yes	4	118d 08:58:53
sfpplus2_cabase	45....	E4:8D:...	r1...	MikroTik	6.48.1 (stable)	CCR1009-8G-1S-1S+	yes	6	46d 10:29:41
sfpplus2_cabase	45....	E4:8D:...	T...	MikroTik	6.48.3 (stable)	CCR1036-8G-2S+	yes	54	109d 18:30:12
sfpplus2_cabase		74:4D:...	C...	MikroTik	6.48.6 (long-term)	CRS328-4C-20S-4S+	no	20	109d 18:33:14
sfpplus2_cabase	200...	74:4D:...	n...	MikroTik	6.49.4 (stable)	CCR1072-1G-8S+	no	44	50d 23:12:47
sfpplus2_cabase	200...	48:8F:5...	IX...	MikroTik	6.49.6 (stable)	CCR1072-1G-8S+	yes	23	109d 18:30:32
sfpplus2_cabase	200...	48:8F:5...	IX...	MikroTik	6.49.6 (stable)	CCR1072-1G-8S+	yes	23	109d 18:30:32
sfpplus2_cabase	200...	74:4D:...	R...	MikroTik	6.49.6 (stable)	CCR1016-12S-1S+	no	3	109d 18:33:15
sfpplus2_cabase	200...	74:4D:...	R...	MikroTik	6.49.6 (stable)	CCR1072-1G-8S+	no	28	71d 18:54:43
sfpplus2_cabase	200...	74:4D:...	R...	MikroTik	6.49.6 (stable)	CCR1072-1G-8S+	no	28	71d 18:54:43
sfpplus2_cabase	200...	74:4D:...	B...	MikroTik	6.49.7 (stable)	CCR1072-1G-8S+	yes	37	135d 16:16:20
sfpplus2_cabase	200...	2C:C8:...	R...	MikroTik	6.49.7 (stable)	CCR1072-1G-8S+	yes	24	87d 04:17:03
sfpplus2_cabase	200...	2C:C8:...	R...	MikroTik	6.49.7 (stable)	CCR1072-1G-8S+	yes	44	357d 05:06:57
sfpplus2_cabase	200...	C4:AD:...	R...	MikroTik	6.49.7 (stable)	CCR1072-1G-8S+	yes	31	109d 18:32:57
sfpplus2_cabase	200...	C4:AD:...	R...	MikroTik	6.49.7 (stable)	CCR1072-1G-8S+	yes	31	109d 18:32:57
sfpplus2_cabase	200...	DC:2C:...	c...	MikroTik	6.49.7 (stable)	CCR1036-8G-2S+	yes	2	108d 03:50:25
sfpplus2_cabase	200...	48:8F:5...	P...	MikroTik	6.49.8 (stable)	CCR1072-1G-8S+	yes	51	102d 11:44:57
sfpplus2_cabase		4C:5E:...	M...	MikroTik	6.49.10 (long-term)	CCR1036-8G-2S+	yes	29	148d 16:44:09
sfpplus2_cabase	45....	2C:C8:...	W...	MikroTik	6.49.10 (long-term)	CCR2004-1G-12S+2XS	yes	46	39d 20:45:23
sfpplus2_cabase	200...	6C:3B:...	Li...	MikroTik	6.49.10 (stable)	CCR1036-8G-2S+	no	50	109d 18:31:24
sfpplus2_cabase	200...	DC:2C:...	rt...	MikroTik	6.49.13 (long-term)	CCR1036-8G-2S+	yes	29	5d 04:41:49
sfpplus2_cabase	200...	DC:2C:...	B...	MikroTik	6.49.13 (stable)	CCR1072-1G-8S+	yes	43	37d 07:11:41
sfpplus2_cabase	200...	48:A9:...	N...	MikroTik	7.10 (stable) Jun/...	CCR2216-1G-12XS-2XQ	yes	40	24d 10:03:12
sfpplus2_cabase	172...	C4:AD:...	s...	MikroTik	7.11 (stable) Aug/...	CRS317-1G-16S+	yes	59	109d 18:30:52
sfpplus2_cabase	172...	C4:AD:...	s...	MikroTik	7.11 (stable) Aug/...	CRS317-1G-16S+	yes	59	109d 18:30:52
sfpplus2_cabase		DC:2C:...	s...	MikroTik	7.11.2 (stable) Au...	CRS317-1G-16S+	yes	53	18d 11:25:57
sfpplus2_cabase		2C:C8:...	s...	MikroTik	7.11.2 (stable) Au...	CRS317-1G-16S+	yes	0	130d 13:10:05
sfpplus2_cabase		2C:C8:...	s...	MikroTik	7.11.2 (stable) Au...	CRS317-1G-16S+	yes	0	130d 13:10:05
sfpplus2_cabase	192...	DC:2C:...	s...	MikroTik	7.11.2 (stable) Au...	CRS317-1G-16S+	yes	53	18d 11:25:57
sfpplus2_cabase	200...	E4:8D:...	C...	MikroTik	7.11.2 (stable) Au...	CCR1036-8G-2S+	yes	51	4d 19:01:29
sfpplus2_cabase	200...	48:A9:...	ro...	MikroTik	7.11.2 (stable) Au...	CCR2216-1G-12XS-2XQ	yes	22	109d 18:31:40

51 items out of 62

- Si ejecutamos un /ip neighbor print en una interfaz conectada al IXP tendremos conocimiento de los dispositivos que corren MNDP o LLDP junto con la versión de software.
- Aún tenemos que hacer pasar por un login para acceder al equipamiento descubierto.
- Algunas versiones antiguas de RouterOS tienen vulnerabilidades que permiten acceso sin login (**CVE-2018-14847** y **CVE-2023-30799**).

MNDP - MikroTik Neighbor Discovery protocol

Aproximaciones para proteger el servicio MNDP/LLDP:

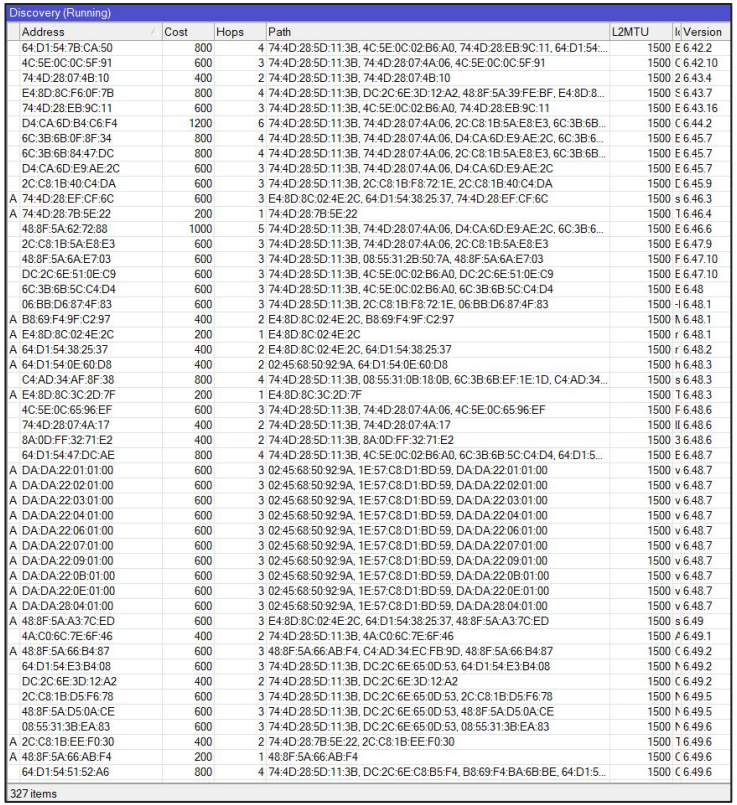
- Sólo permitir descubrimiento en interfaces de gestión y/o backbone:

```
/interface list add name=ilist_discovery
/interface list member add interface=sfpplus2_backbone name=ilist_discovery
/interface list member add interface=vlan999_mgmt name=ilist_discovery
/ip neighbor discovery-settings set discover-interface-list=ilist_discovery

#Opcional

/ip neighbor discovery-settings set mode=rx-only
```

ROMON - Router Management Overlay Network



Discovery (Running)

	Address	Cost	Hops	Path	L2MTU	I	Version
	64:D1:54:7B:CA:50	800	4	74:4D:28:5D:11:3B, 4C:5E:0C:02:B6:A0, 74:4D:28:EB:9C:11, 64:D1:54:...	1500	E	6.42.2
	4C:5E:0C:0C:5F:91	600	3	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, 4C:5E:0C:0C:5F:91	1500	C	6.42.10
	74:4D:28:07:4B:10	400	2	74:4D:28:5D:11:3B, 74:4D:28:07:4B:10	1500	2	6.43.4
	E4:8D:8C:F6:0F:7B	800	4	74:4D:28:5D:11:3B, DC:2C:6E:3D:12:A2, 48:8F:5A:39:FE:BF, E4:8D:8...	1500	S	6.43.7
	74:4D:28:EB:9C:11	600	3	74:4D:28:5D:11:3B, 4C:5E:0C:02:B6:A0, 74:4D:28:EB:9C:11	1500	E	6.43.16
	D4:CA:6D:B4:C6:F4	1200	6	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, 2C:C8:1B:5A:E8:E3, 6C:3B:6B...	1500	C	6.44.2
	6C:3B:6B:0F:8F:34	800	4	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, D4:CA:6D:E9:AE:2C, 6C:3B:6...	1500	E	6.45.7
	6C:3B:6B:84:47:DC	800	4	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, 2C:C8:1B:5A:E8:E3, 6C:3B:6B...	1500	E	6.45.7
	D4:CA:6D:E9:AE:2C	600	3	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, D4:CA:6D:E9:AE:2C	1500	E	6.45.7
	2C:C8:1B:40:C4:DA	600	3	74:4D:28:5D:11:3B, 2C:C8:1B:F8:72:1E, 2C:C8:1B:40:C4:DA	1500	D	6.45.9
A	74:4D:28:EF:CF:6C	600	3	E4:8D:8C:02:4E:2C, 64:D1:54:38:25:37, 74:4D:28:EF:CF:6C	1500	s	6.46.3
A	74:4D:28:7B:5E:22	200	1	74:4D:28:7B:5E:22	1500	T	6.46.4
	48:8F:5A:62:72:88	1000	5	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, D4:CA:6D:E9:AE:2C, 6C:3B:6...	1500	E	6.46.6
	2C:C8:1B:5A:E8:E3	600	3	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, 2C:C8:1B:5A:E8:E3	1500	E	6.47.9
	48:8F:5A:6A:E7:03	600	3	74:4D:28:5D:11:3B, 08:55:31:2B:50:7A, 48:8F:5A:6A:E7:03	1500	F	6.47.10
	DC:2C:6E:51:0E:C9	600	3	74:4D:28:5D:11:3B, 4C:5E:0C:02:B6:A0, DC:2C:6E:51:0E:C9	1500	E	6.47.10
	6C:3B:6B:5C:C4:D4	600	3	74:4D:28:5D:11:3B, 4C:5E:0C:02:B6:A0, 6C:3B:6B:5C:C4:D4	1500	E	6.48
	06:BB:D6:87:4F:83	600	3	74:4D:28:5D:11:3B, 2C:C8:1B:F8:72:1E, 06:BB:D6:87:4F:83	1500	-	6.48.1
A	B8:69:F4:9F:C2:97	400	2	E4:8D:8C:02:4E:2C, B8:69:F4:9F:C2:97	1500	M	6.48.1
A	E4:8D:8C:02:4E:2C	200	1	E4:8D:8C:02:4E:2C	1500	r	6.48.1
A	64:D1:54:38:25:37	400	2	E4:8D:8C:02:4E:2C, 64:D1:54:38:25:37	1500	r	6.48.2
A	64:D1:54:0E:60:D8	400	2	02:45:68:50:92:9A, 64:D1:54:0E:60:D8	1500	h	6.48.3
	C4:AD:34:AF:8F:38	800	4	74:4D:28:5D:11:3B, 08:55:31:0B:18:0B, 6C:3B:6B:EF:1E:1D, C4:AD:34...	1500	s	6.48.3
A	E4:8D:8C:3C:2D:7F	200	1	E4:8D:8C:3C:2D:7F	1500	T	6.48.3
	4C:5E:0C:65:96:EF	600	3	74:4D:28:5D:11:3B, 74:4D:28:07:4A:06, 4C:5E:0C:65:96:EF	1500	F	6.48.6
	74:4D:28:07:4A:17	400	2	74:4D:28:5D:11:3B, 74:4D:28:07:4A:17	1500	ll	6.48.6
	8A:0D:FF:32:71:E2	400	2	74:4D:28:5D:11:3B, 8A:0D:FF:32:71:E2	1500	3	6.48.6
	64:D1:54:47:DC:AE	800	4	74:4D:28:5D:11:3B, 4C:5E:0C:02:B6:A0, 6C:3B:6B:5C:C4:D4, 64:D1:5...	1500	E	6.48.7
A	DA:DA:22:01:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:01:01:00	1500	v	6.48.7
A	DA:DA:22:02:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:02:01:00	1500	v	6.48.7
A	DA:DA:22:03:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:03:01:00	1500	v	6.48.7
A	DA:DA:22:04:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:04:01:00	1500	v	6.48.7
A	DA:DA:22:06:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:06:01:00	1500	v	6.48.7
A	DA:DA:22:07:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:07:01:00	1500	v	6.48.7
A	DA:DA:22:09:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:09:01:00	1500	v	6.48.7
A	DA:DA:22:0B:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:0B:01:00	1500	v	6.48.7
A	DA:DA:22:0E:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:22:0E:01:00	1500	v	6.48.7
A	DA:DA:28:04:01:00	600	3	02:45:68:50:92:9A, 1E:57:C8:D1:BD:59, DA:DA:28:04:01:00	1500	v	6.48.7
A	48:8F:5A:A3:7C:ED	600	3	E4:8D:8C:02:4E:2C, 64:D1:54:38:25:37, 48:8F:5A:A3:7C:ED	1500	s	6.49
	4A:C0:6C:7E:6F:46	400	2	74:4D:28:5D:11:3B, 4A:C0:6C:7E:6F:46	1500	A	6.49.1
A	48:8F:5A:66:B4:87	600	3	48:8F:5A:66:AB:F4, C4:AD:34:EC:FB:9D, 48:8F:5A:66:B4:87	1500	C	6.49.2
	64:D1:54:E3:B4:08	600	3	74:4D:28:5D:11:3B, DC:2C:6E:65:0D:53, 64:D1:54:E3:B4:08	1500	N	6.49.2
	DC:2C:6E:3D:12:A2	400	2	74:4D:28:5D:11:3B, DC:2C:6E:3D:12:A2	1500	C	6.49.2
	2C:C8:1B:D5:F6:78	600	3	74:4D:28:5D:11:3B, DC:2C:6E:65:0D:53, 2C:C8:1B:D5:F6:78	1500	N	6.49.5
	48:8F:5A:D5:0A:CE	600	3	74:4D:28:5D:11:3B, DC:2C:6E:65:0D:53, 48:8F:5A:D5:0A:CE	1500	N	6.49.5
	08:55:31:3B:EA:83	600	3	74:4D:28:5D:11:3B, DC:2C:6E:65:0D:53, 08:55:31:3B:EA:83	1500	N	6.49.6
A	2C:C8:1B:EE:F0:30	400	2	74:4D:28:7B:5E:22, 2C:C8:1B:EE:F0:30	1500	T	6.49.6
A	48:8F:5A:66:AB:F4	200	1	48:8F:5A:66:AB:F4	1500	C	6.49.6
	64:D1:54:51:52:A6	800	4	74:4D:28:5D:11:3B, DC:2C:6E:C8:B5:F4, B8:69:F4:BA:6B:BE, 64:D1:5...	1500	C	6.49.6

327 items

- Si ejecutamos un /tool romon discover en una interfaz conectada al IXP tendremos conocimiento de las redes que tienen ROMON activo con configuración por defecto.
- Aún tenemos que hacer pasar por un login para acceder al equipamiento descubierto.
- Algunas versiones antiguas de RouterOS tienen vulnerabilidades que pueden ser explotadas (ver cve.org o shodan.io).

ROMON - Router Management Overlay Network

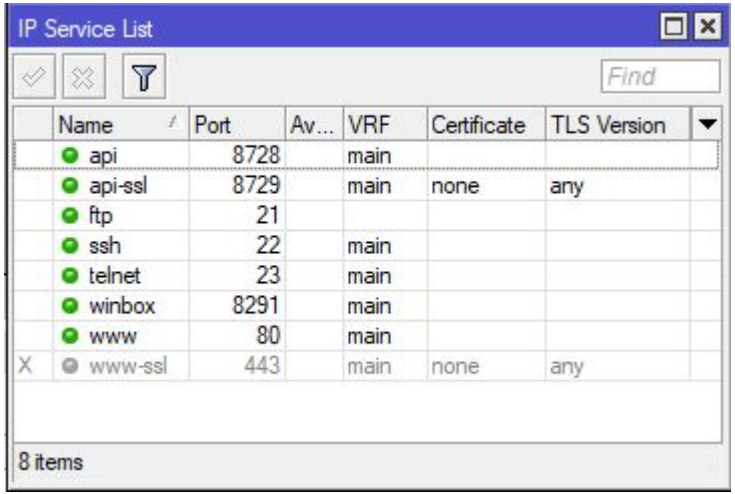
Aproximaciones para proteger el servicio ROMON:

- Sólo permitir descubrimiento en interfaces de gestión y/o backbone:

```
/tool romon port set [find interface=all] forbid=yes
/tool romon port add interface=sfpplus2_backbone disabled=no
/tool romon port add interface=vlan999_mgmt disabled=no
/tool romon set secrets=12345678
/tool romon set enabled=yes
```

- Sólo permitir acceso al servicio ROMON (TCP 8291) a IPs conocidas o confiables (ver sección Firewall).

Servicios de acceso

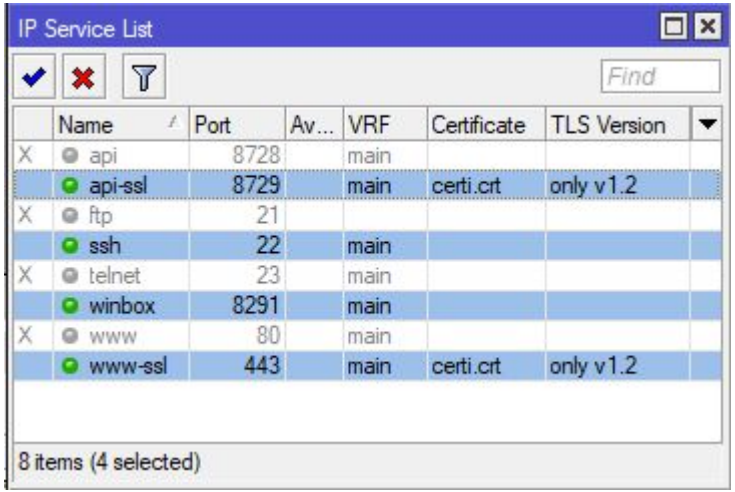


Servicios sin cifrado y con autenticación en texto plano o vulnerable:

- ❏ API
- ❏ FTP
- ❏ Telnet
- ❏ WWW (WebFig)

Recomendación: deshabilitar!

Servicios de acceso



Aproximaciones: dejar sólo servicios con cifrado y autenticación segura.

- **API-SSL**: agregar certificado y usar TLS 1.2.
- **WWW-SSL**: agregar certificado y usar TLS 1.2.
- **WinBox**: proteger desde /ip firewall
- **SSH**: mejorar seguridad desde /ip ssh

Servicios de acceso

- Mejorar el servicio SSH:

```
/ip ssh
set strong-crypto=yes
set host-key-type=ed25519
```

- Mejorar el servicio WinBox:

  Implementar técnica Port Knocking.

Firewall “cero confianza” (zero trust)

- Es recomendable proteger el router con un Firewall que descarte todo. El tráfico permitido debería ser declarado de forma explícita con una regla:

```
/ip firewall filter
add comment="Permitir paquetes de conexiones establecidas" \
    chain=input connection-state=established action=accept
add comment="Permitir todo desde alist_gestion" \
    chain=input src-address-list=alist_gestion action=accept
add comment="Descartar todo" \
    chain=input action=drop log=no log-prefix=DESCARTADO:
```

Firewall que cumpla con BCP38

- Es recomendable cumplir con BCP38!

```
/ip firewall raw
add comment="Para cumplir con BCP38" \
    chain=prerouting  \
    in-interface-list=ilist_acceso \
    src-address-list=!alist_redes-acceso \
    action=drop
```

Accesos VPN

- VPN inseguras y sus reemplazos:
  - **PPTP** se reemplaza con **SSTP** y certificados.
  - **L2TP** se potencia agregando una llave **IPsec**.

- Otras VPN seguras soportadas por RouterOSv7:
  - **OpenVPN**, se mejora la performance con el modo UDP.
  - **WireGuard**, mejora la seguridad y performance.

PROZCENTER
CENTRO DE PROFESIONALES

¡Muchas gracias!

Seguridad y BGP en RouterOS v7

Mayo 2024, CABA

CÁMARA ARGENTINA DE Internet

XX Encuentro Nacional de Técnicos