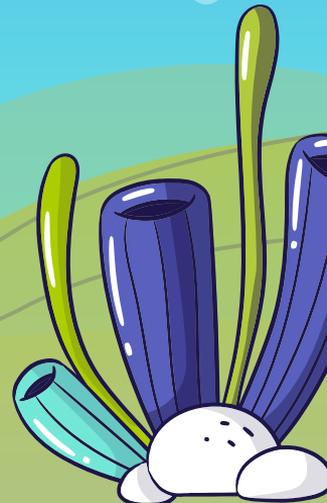




COMO MIKROTIK ARRUINÓ MI VIDA

De la droga se sale,
de Mikrotik NO





¿QUIEN ES ESTE TÍO?

DE GRANÁ

Trabajo en DMNTR Network Solutions

Soluciones de Red - Ciberseguridad

Escribo historias por Twitter, envío una Newsletter semanal y algunos días cuento cosas en un podcast mientras voy al trabajo



DMNTR
NETWORK SOLUTIONS



¿DE QUE VAMOS A HABLAR?

01

EL PRINCIPIO

Todo empezó con antenas...

MITM

Pero había demasiada gente en medio...

02

03

¡NO SE PUEDE!

Felipe lo que quieres hacer no se puede hacer...

¡SI SE PUEDE!

¿Que alguien en un podcast dice qué?

04

05

¡QUE SI!

Haters gonna hate



EL PRINCIPIO

Vivíamos en un pueblo

Teníamos un ADSL de 1Mbps

Éramos jóvenes e inexpertos...



EL PRINCIPIO

Vivíamos en un pueblo

Teníamos un ADSL de 1Mbps

Éramos jóvenes e inexpertos...



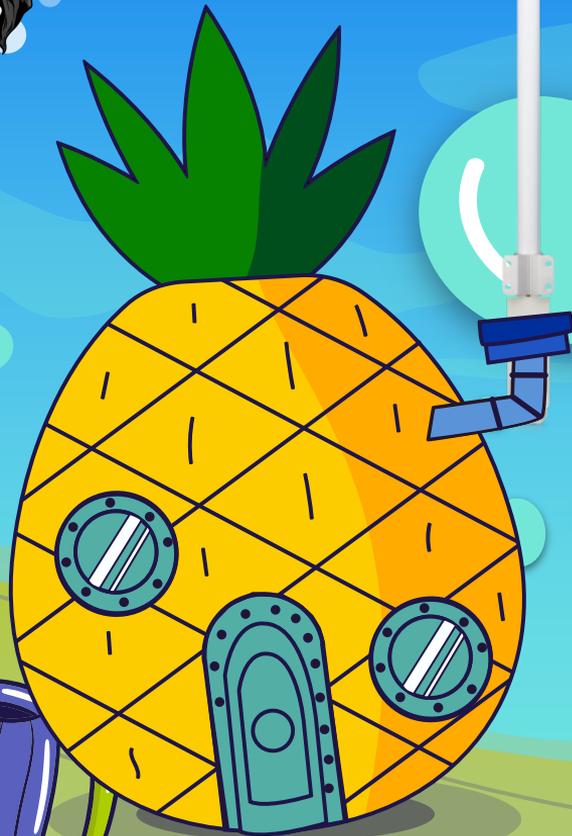
EL PRINCIPIO

Azahara Fernández

para Felipe

24/6/09

A la casa nos llegan los 10Mb de Telefonica, podemos contratarlo y vender internet otro negocio hay que buscarse la vida, por si aca. ¿Como va tu super pagina?

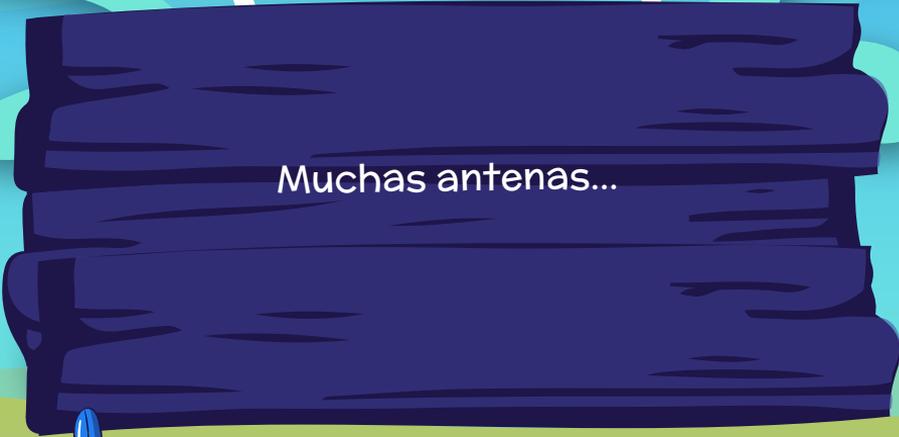


EL PRINCIPIO

Así que Ubiquiti entro en nuestras
vidas y empezamos a poner antenas...



EL PRINCIPIO



Muchas antenas...

EL PRINCIPIO

Muuuuuuuuuuuchas antenas...





EL PRINCIPIO

Pero necesitábamos muchas cosas
como:

Radius, PPPoE, QoS, CG-NAT...



EL PRINCIPIO

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help theutopyfw1.theutopy

Status: Dashboard



Picture

the utopy

free.social.independent.human.



System Information

Interfaces

WAN	↑	172.16.0.100	100baseTX <full-duplex>
LAN	↑	10.0.0.10	100baseTX <full-duplex>

Gateways

Name	Gateway	RTT	Loss	Status
WANGW	172.16.0.1	0.305ms	0.0%	Online

Traffic Graphs

Current WAN Traffic



Current LAN Traffic



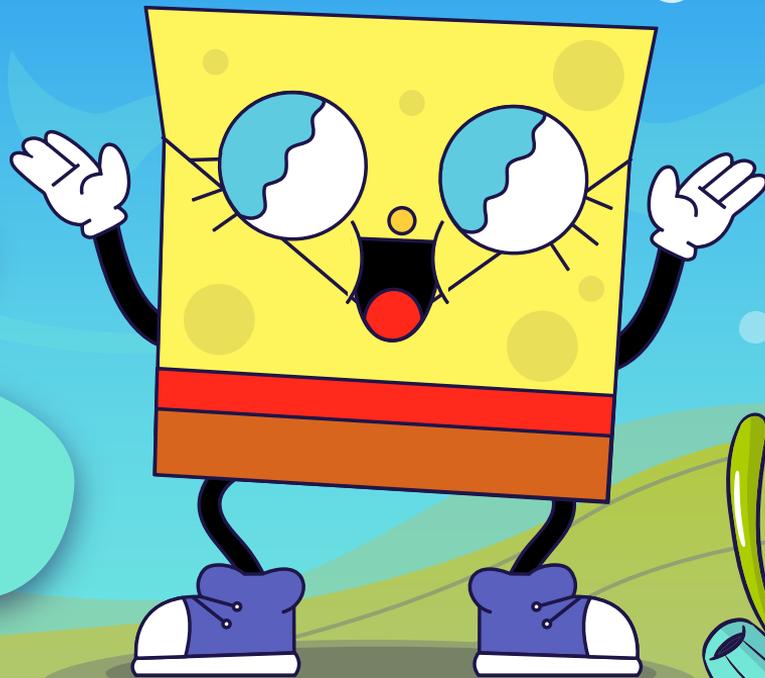
THE FRIENDS

MikroTik



Ubiquiti

Aún no lo sabíamos pero
esto no iba a ser bueno...





MikroTik + Ubiquiti



Aún no lo sabíamos pero
esto no iba a ser bueno...

¡AHORA ERAMOS UN WISP!

- Subíamos en tejados.
- Dábamos asistencia 24/7/365
- Nos llamaban porque el porn iba lento.

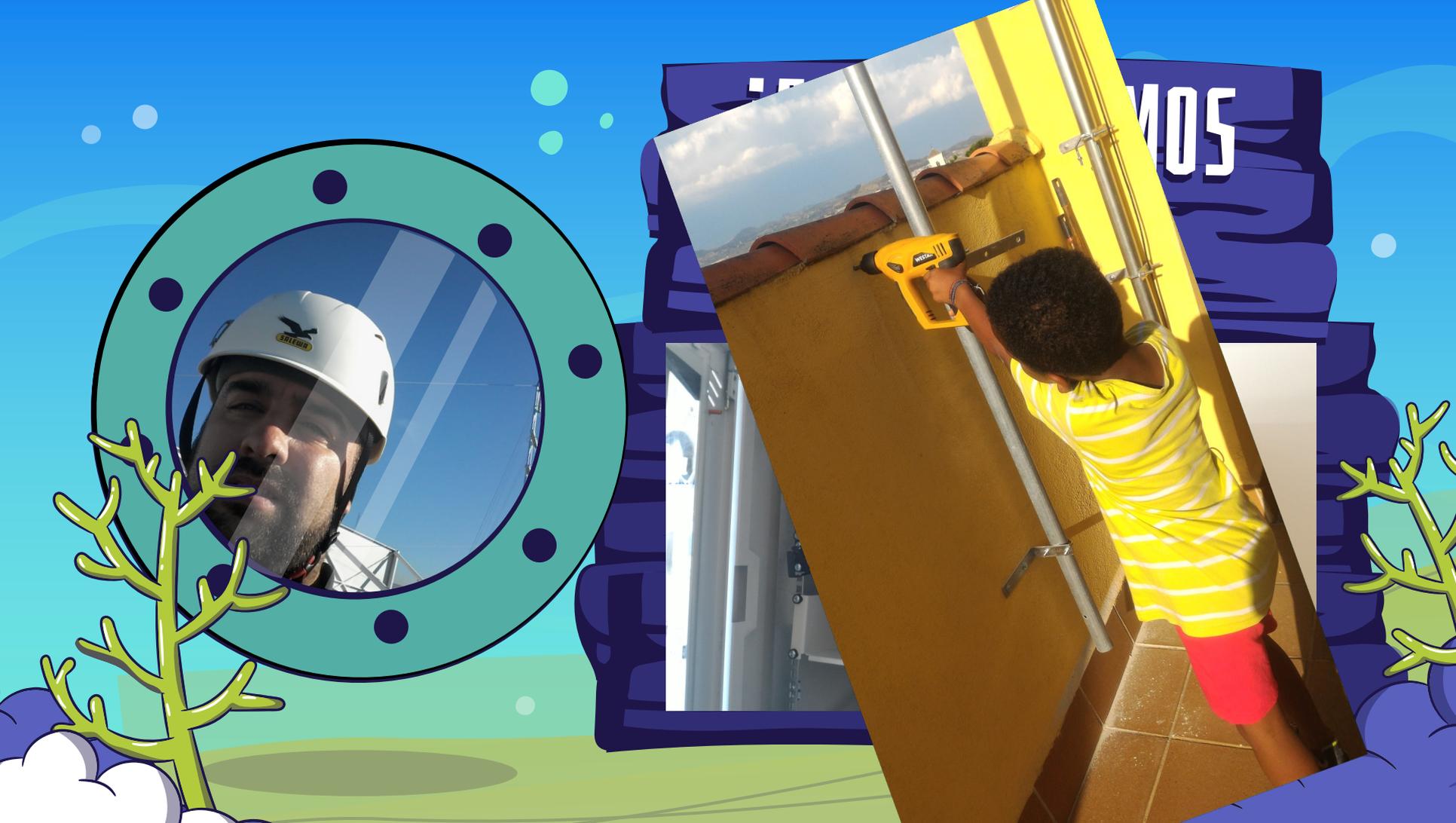
¡Que trabajo mas gratificante!

¡Como no me metí en esto antes!



¡AHORA ERAMOS
UN WISP!









Felipe Cañizares

having successfully completed the appropriate training and certification requirements, is hereby recognised as a MikroTik certified

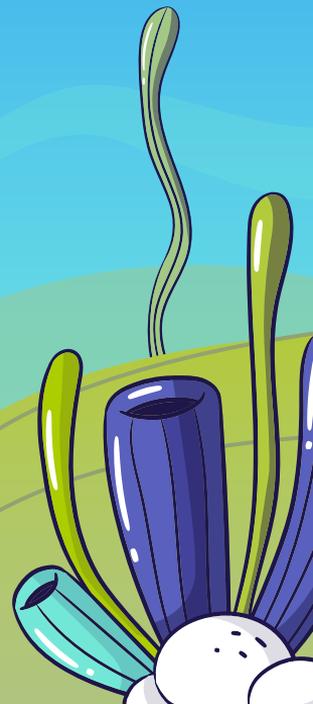
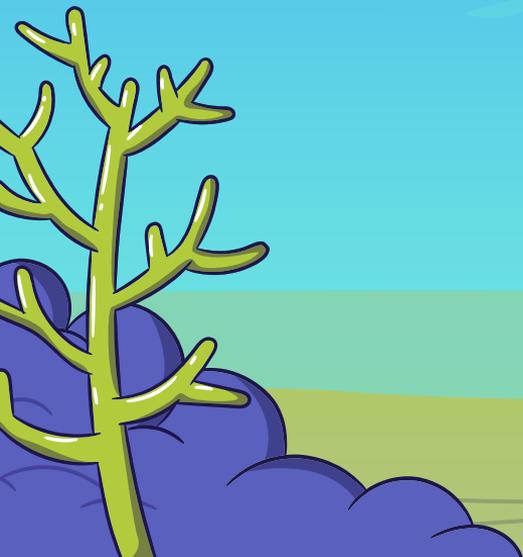
MTCNA

#1311NA411

20-11-2013

Valid for three years since issue. Validate the authenticity of this document at <http://www.mikrotik.com/certificates/>
Issued by MikroTiks SIA, Pernavas 46, Riga, Latvia

MITM



MITM



PROBLEMAS

No teníamos IPs propias
Si fallaba el caudal... ¡Adios!
Era difícil crecer...

¡Aún tenía algo de tiempo libre!



SOLUCIONES

¿Y si nos quitamos al Man in
the Middle y llevamos el ISP
hasta el siguiente nivel?

¡VAMOS A HACERNOS LIR!

MITM



PROBLEMAS

Eso del LIR no es fácil...
La web del RIPE está en inglés
¿BGqué?

Esto lo vi yo en la carrera...
¿Qué se han agotado las Ips?



SOLUCIONES

Toca estudiar todo esto o
bien preguntar a otra gente...

¡Y a mi estudiar nunca me ha
gustado!

¡NO SE PUEDE!



EL DE CISCO

¡Eso no se
puede hacer
con Mikrotik!

EL DE JUNIPER

¡Eso no se
puede hacer
con Churrotik!

EL OTRO

¡Eso no se
puede hacer!

¡NO SE PUEDE!

2018

Pues no se puede...

2019

Que difícil es eso de
BGP...

2020

Que no... que no se
puede...

2021

DMNTR
¿Eduardo Collado?
¿Javi-H?

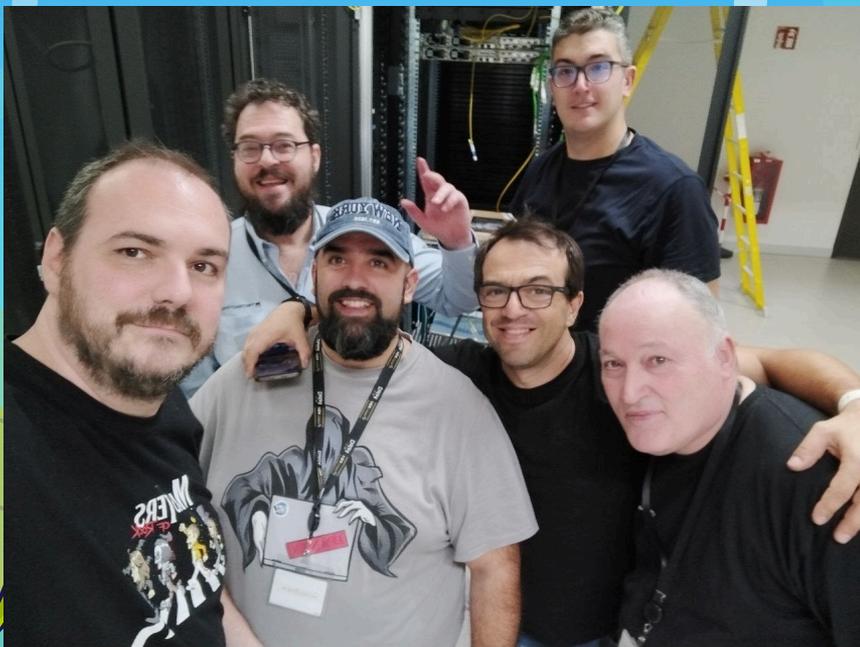
2022

¡QUE SOMOS LIR!
¡Y tenemos IPv6!

2023

¡Y ahora hasta tenemos
IPv4!

LO MISMO... SE PUEDE...



TECNOCRÁTICA

¡ PUES SI SE PUEDE !



¡ PUES SI SE PUEDE !



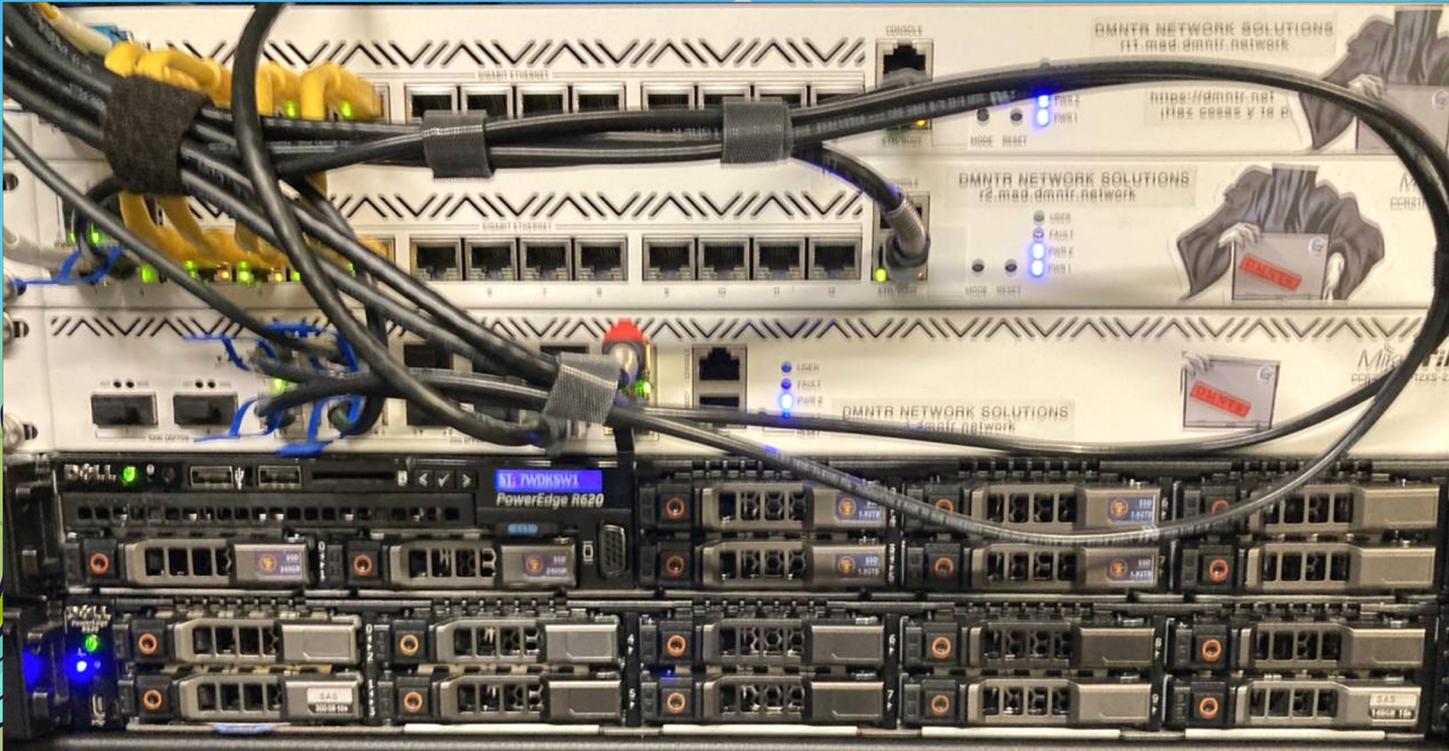
¡ PUES SI SE PUEDE !



¡ PUES SI SE PUEDE !



¡ PUES SI SE PUEDE !



¡ PUES SI SE PUEDE !

Route Filters

Rule Select Rule Num Set Community Set Community Ext Set Community Large Set



#	Chain	Rule
		;;; Miramos si hay un blackhole, si no, seguimos...
1	decixrsv6_in	jump IN_BHOLEv6
		;;; Seteamos local-preference y desactivamos BGP-MED
50	decixrsv6_in	set bgp-local-pref 130; unset bgp-med
		;;; Validamos RPKI
51	decixrsv6_in	jump IN_RPKI
		;;; Miramos si hay un graceful shutdown, si no, seguimos...
52	decixrsv6_in	jump IN_GRACEFUL_SHUTDOWN
		;;; Aceptamos el resto
53	decixrsv6_in	accept

¡ PUES SI SE PUEDE !

RFC 8326

Graceful BGP Session Shutdown,

Route Filters

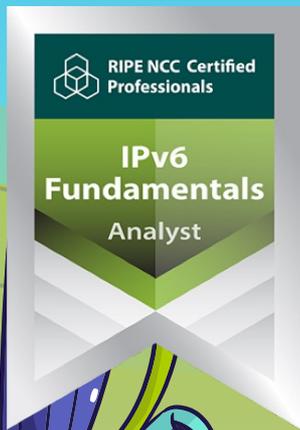
Rule	Select Rule	Num Set	Community Set	Community Ext Set	Community Large Set
					
#	Chain	Rule			
		;;; 65535:0 -> LOCAL PREFERENCE 0 (Para mantenimientos de routers o del peering, nos tiran las rutas antes del mantenimiento)			
60	IN_GRACEFUL_SHUTDOWN	if (bgp-communities includes 65535:0) { set bgp-local-pref 0; accept }			
		;;; A la siguiente regla...			
61	IN_GRACEFUL_SHUTDOWN	return			

¡ PUES SI SE PUEDE !



RIPE NCC

Member



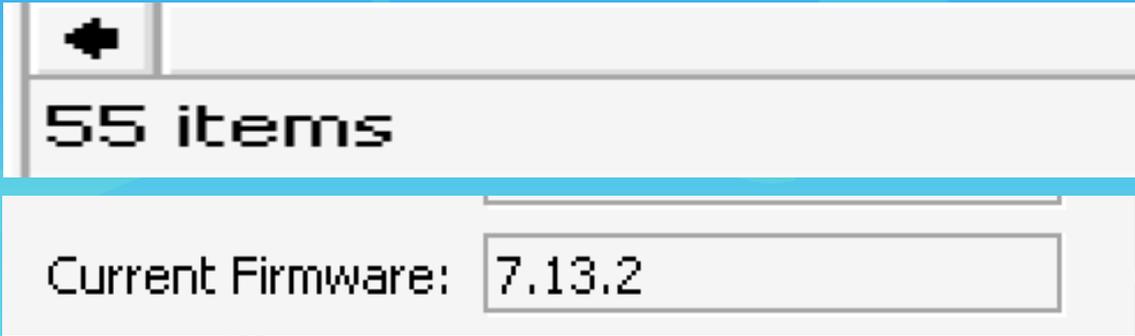
DE CIX MANRS

¡ PUES SI SE PUEDE !



BGP Configuration Window showing a list of connections:

Name	Template	AFI
Peering-PCH4-1	peeringv4	ip
Peering-PCH6-1	peeringv6	ipv6
Peering-Netflix4-1	peeringv4	ip
Peering-Netflix4-2	peeringv4	ip
Peering-Netflix6-1	peeringv6	ipv6
Peering-Netflix6-2	peeringv6	ipv6
Peering-PCH4-2	peeringv4	ip
Peering-PCH6-2	peeringv6	ipv6
Peering-CPRM4	peeringv4	ip
Peering-CPRM6	peeringv6	ipv6
Peering-DIGI4-1	peeringv4	ip
Peering-DIGI4-2	peeringv4	ip
Peering-DIGI6-1	peeringv6	ipv6
Peering-DIGI6-2	peeringv6	ipv6
Peering-Yahoo4-1	peeringv4	ip
Peering-Yahoo4-2	peeringv4	ip
Peering-Yahoo6-1	peeringv6	ipv6
Peering-Yahoo6-2	peeringv6	ipv6
Peering-Cloudflare4	peeringv4	ip
Peering-Cloudflare6	peeringv6	ipv6
Peering-Twitter4	peeringv4	ip
Peering-Twitter6	peeringv6	ipv6
Peering-Edgio4	peeringv4	ip
Peering-Edgio6	peeringv6	ipv6
Peering-Google4	peeringv4	ip
Peering-Google6	peeringv6	ipv6
Peering-Masmovil4	peeringv4	ip
Peering-OWH4	peeringv4	ip
Peering-OWH6	peeringv6	ipv6
Peering-Amazon4-1	peeringv4	ip
Peering-Amazon4-2	peeringv4	ip
Peering-Amazon6-1	peeringv6	ipv6
Peering-Amazon6-2	peeringv6	ipv6
Peering-Akamai4	peeringv4	ip
Peering-Akamai6	peeringv6	ipv6
Peering-Meta4-1	peeringv4	ip
Peering-Meta4-2	peeringv4	ip
Peering-Meta6-1	peeringv6	ipv6
Peering-Meta6-2	peeringv6	ipv6
Peering-Twitch4-1	peeringv4	ip
Peering-Twitch4-2	peeringv4	ip
Peering-Twitch6-1	peeringv6	ipv6
Peering-Twitch6-2	peeringv6	ipv6
Decix Route Server 1 IPv4	decix-rsv4	ip
Decix Route Server 2 IPv4	decix-rsv6	ipv6
Decix Route Server 1 IPv6	decix-rsv6	ipv6



¡ PUES SI SE PUEDE !





Y ESTO NOS
CAMBIÓ LA
VIDA

ALGO MAS DE HISTORIA

2019

Apostamos por la
ciberseguridad

2020

Empezamos a jugar
generar threat
intelligence propia...

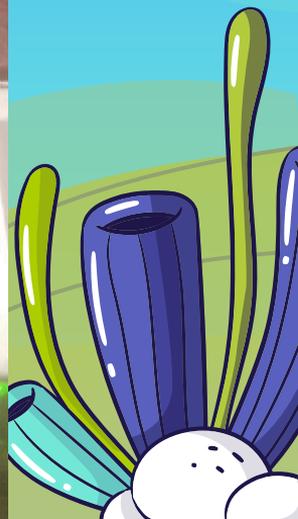
2022

¡EL LIR NOS DA ALAS!
¡Comercializamos
nuestra Blocklist!

2023

Creamos ZEROSET
¡Con Mikrotik!

UN POCO MAS DE HISTORIA



UN POCO MAS DE HISTORIA



¡QUE NO!



EL DE FORTI

¡Eso no se
puede hacer
con Mikrotik!

EL DE WG

¡Eso no se
puede hacer
con Mikrotik!

EL OTRO

¡Eso no se
puede
haceeeeeeeer!

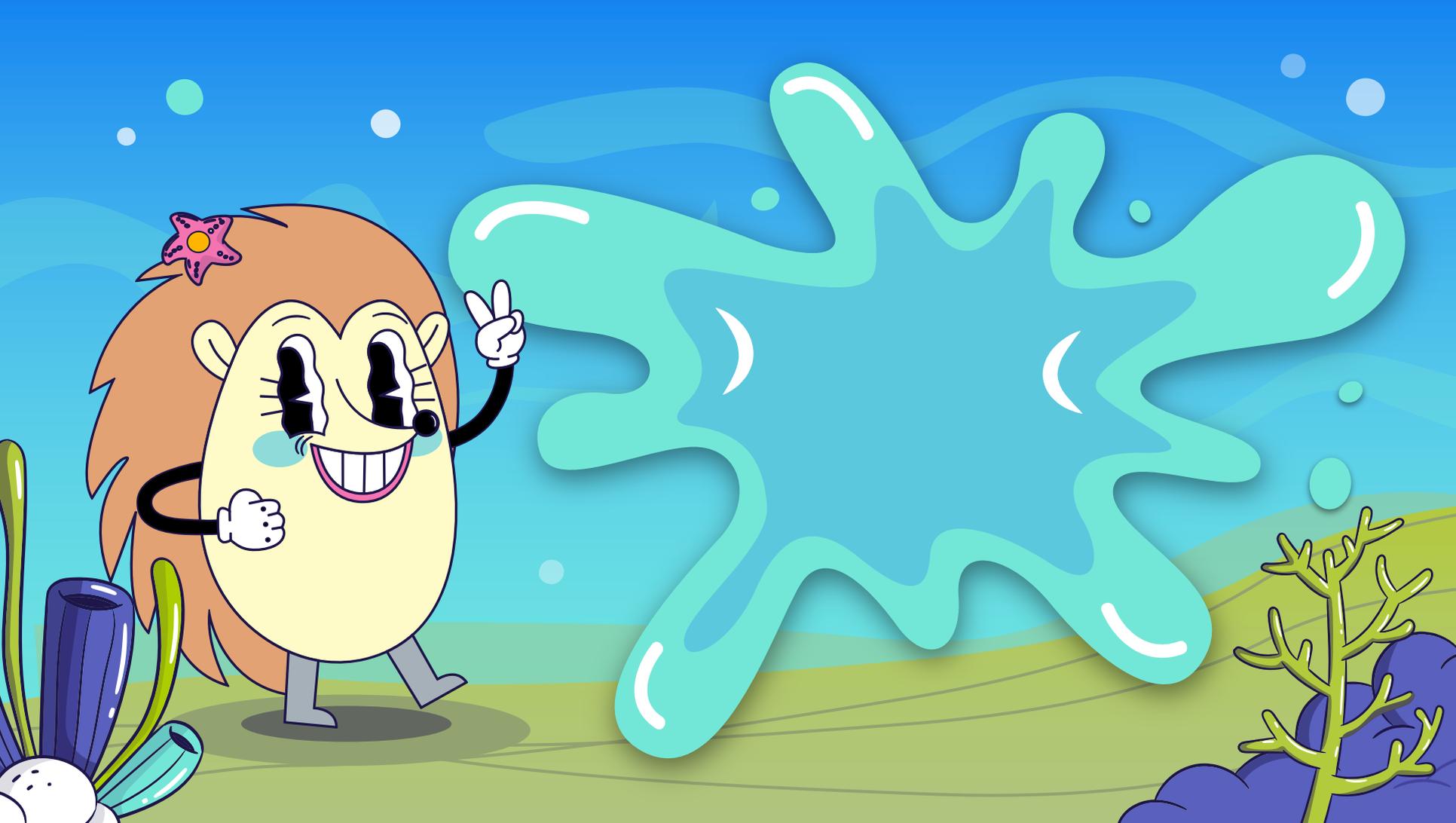
¡QUE SÍ!

IPBLOCK

DNS FILTER

IDS/IPS

ENTRA







Nunca digas a
nadie que no puede
hacer algo y sobre
todo:

**¡NUNCA TE LO
DIGAS A TI MISMO!**



¡GRACIAS!