



SEGURIDAD DE PERÍMETRO CON MIKROTIK

MUM GUATEMALA, ENERO 2020

QUIÉNES SOMOS?

- 3Ds Telecommunications
- Enfoque telemática y ciberseguridad
- San José Costa Rica
- www.3dstelecom.com



3DS
TELECOMMUNICATION

CERTIFICACIONES



3D'S TELECOMMUNICATIONS

- Con más de 20 años de experiencia, nace 3D'S TELECOMMUNICATIONS con la finalidad de brindar soluciones a la medida de tecnologías de la información y comunicaciones, además de enfocarnos otras áreas como la ciberseguridad, redes y diseño gráfico. Ubicados en la zona de los Santos, cantón de Tarrazú y con cobertura a nivel nacional e internacional.



MISIÓN

- Brindar, ayudar y guiar a nuestros clientes a alcanzar sus metas y proyectos de negocio proveyéndoles servicios y soluciones innovadoras acorde a sus necesidades.



VISIÓN

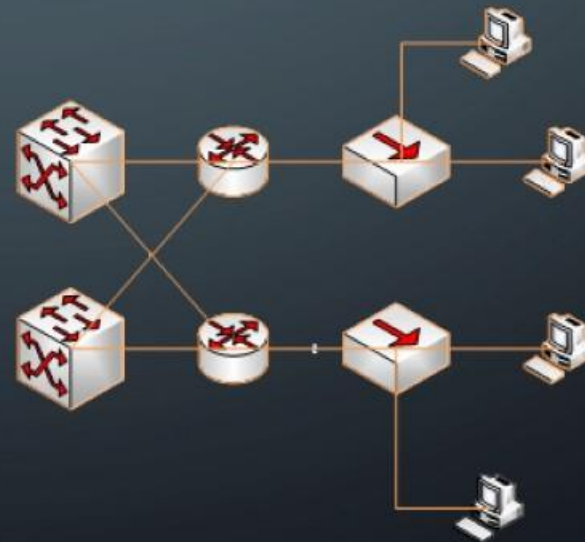
- Ser la compañía en servicios de tecnología informática seleccionada por nuestra innovación, soluciones, productos y servicios. Ser reconocida por la capacidad técnica, calidad humana y profesional de nuestro personal y por nuestra contribución a la comunidad.

EXPERIENCIA

- 20 años en labores de TIC
- Networking (ISP) y TVD
 - Diseño, desarrollo, implementación y mantenimiento red Carrier y backbone Coopesantos R,L.
 - Diseño, desarrollo, implementación y mantenimiento proyecto Televisión Digital Coopesantos R,L.
 - Diseño, desarrollo, implementación y mantenimiento proyecto de seguridad perimetral en la red de Carrier Coopesantos R,L
 - Diseño, desarrollo, implementación y mantenimiento proyecto de seguridad perimetral en la red Apacoop R,L
 - Diseño, desarrollo, implementación y mantenimiento proyecto de la red de la Municipalidad de Dota
- Desarrollo de software e infraestructura
 - Servidores Linux
 - Servidores Microsoft
 - Bases de datos
 - Sistemas a la medida (ERP, Sistemas transaccionales)

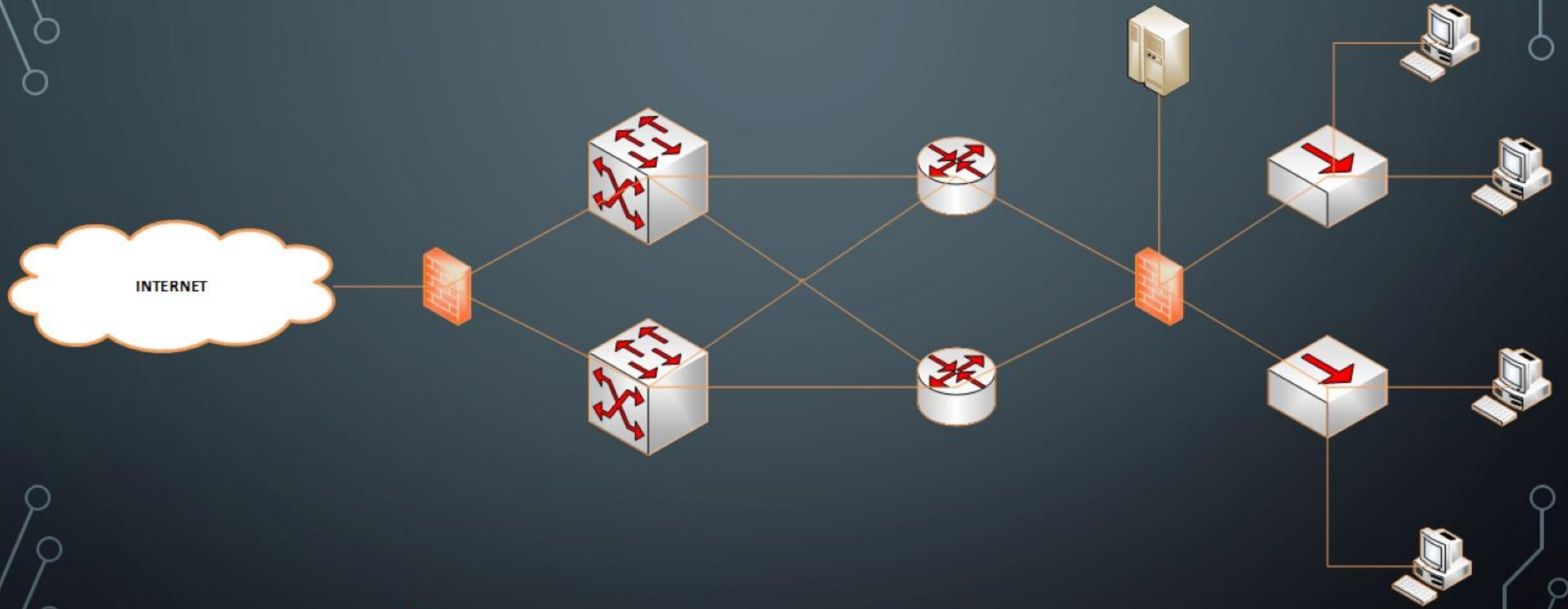
DISEÑO DE CAPAS

- Permite definir la seguridad mediante capas de protección mediante segmentos de red.
- Dicha definición permite la aplicación de seguridad de manera correcta acorde al tráfico de nuestra red.



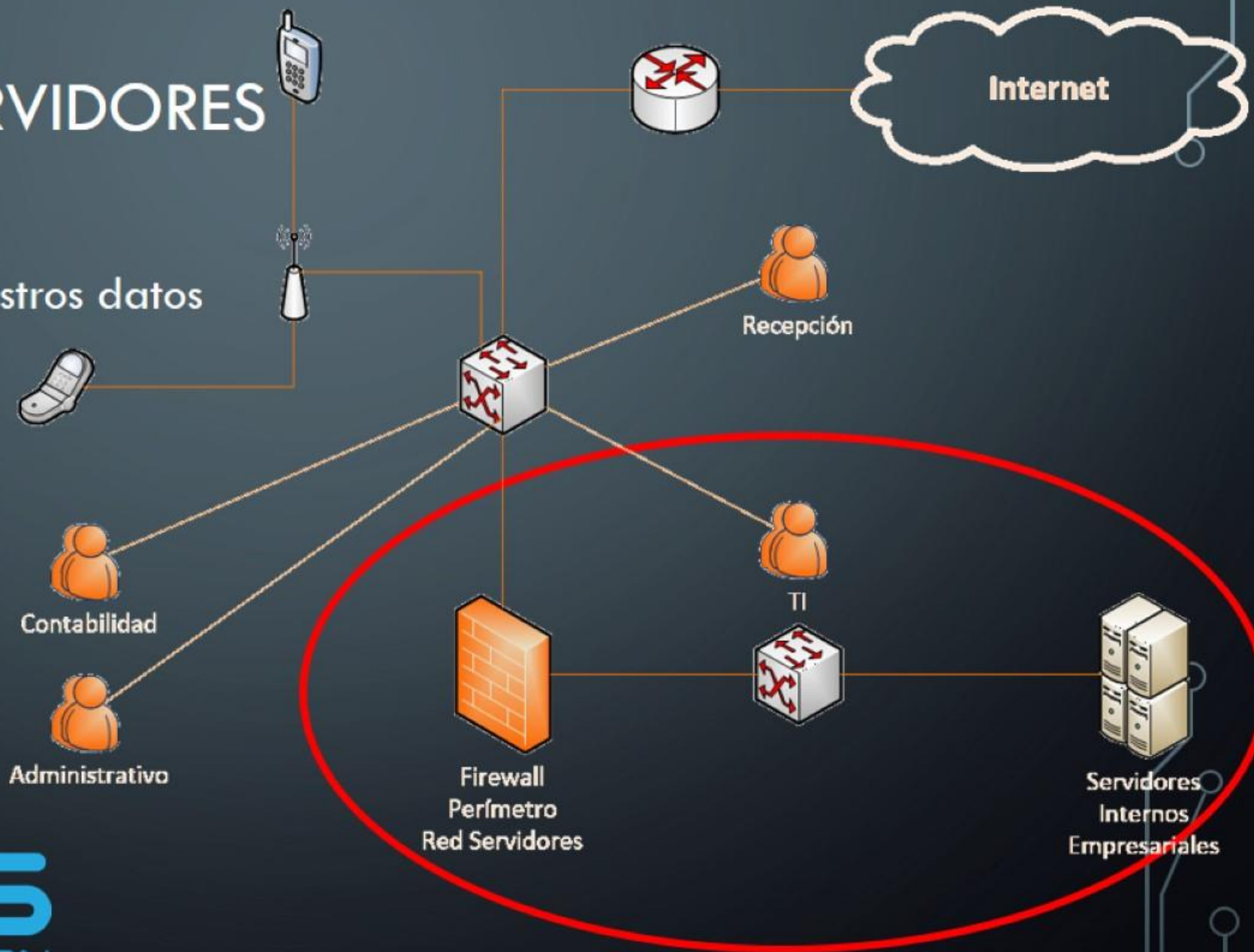
PROTECCIÓN POR CAPAS

- Seguridad en el centro de datos, protección a servidores
- Seguridad en la red interna, corporativa
- Seguridad de perímetro y sucursales



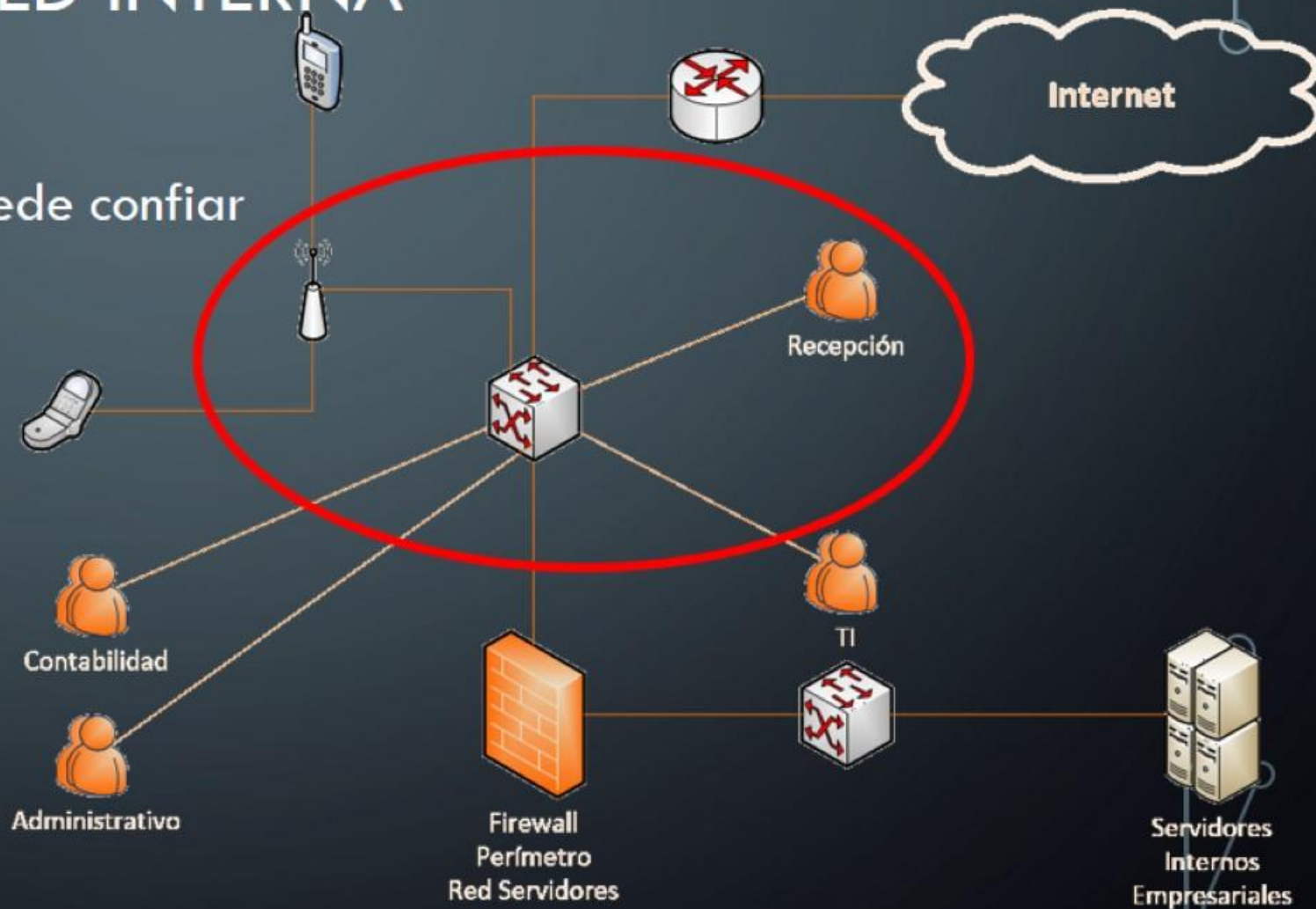
SEGURIDAD SERVIDORES

- La importancia de nuestros datos



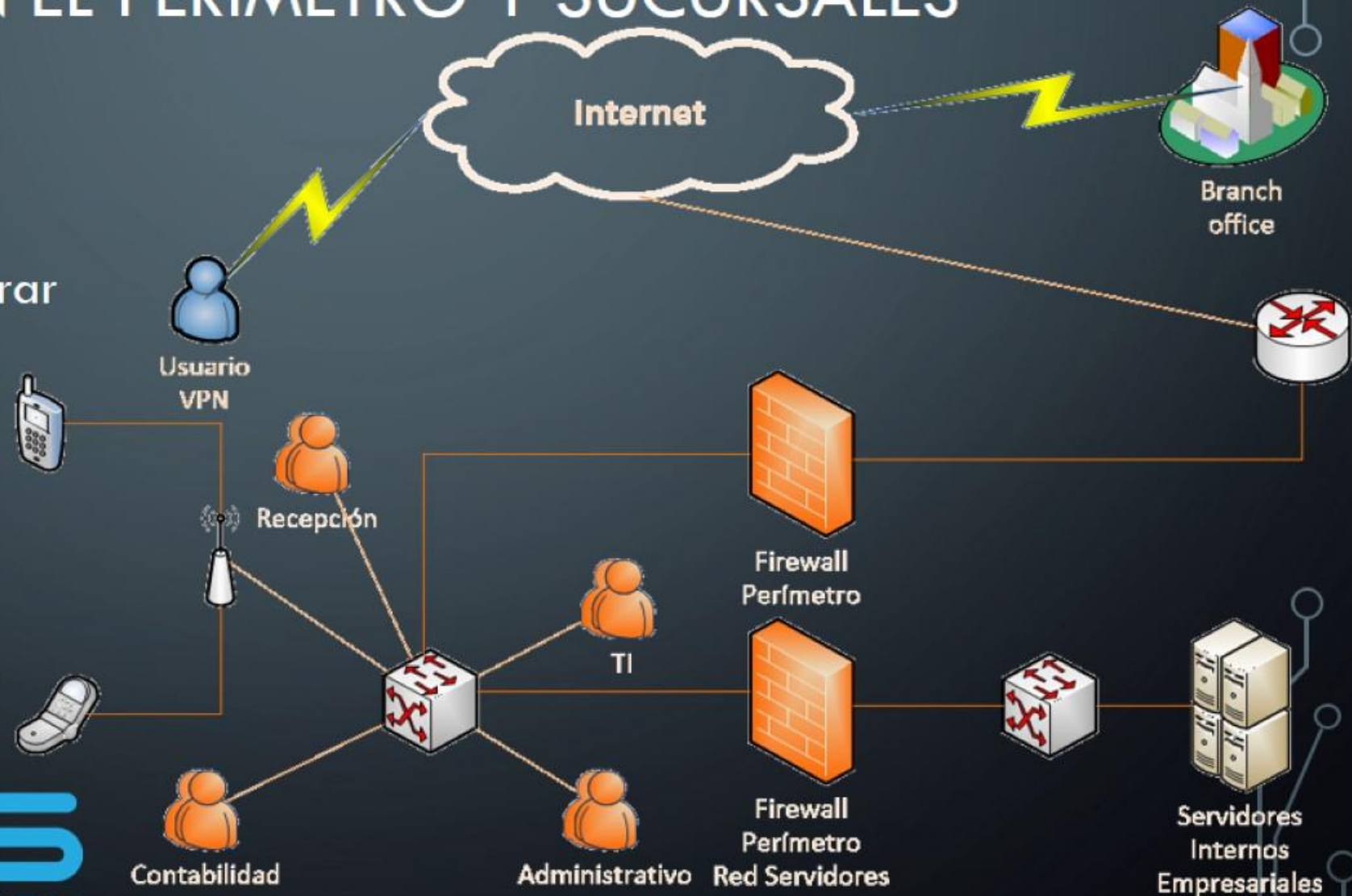
SEGURIDAD EN LA RED INTERNA

- La confianza donde no se puede confiar



SEGURIDAD EN EL PERÍMETRO Y SUCURSALES

- VPN
- Entra quien debe entrar
- IPSEC
 - Excelente seguridad
 - Buen rendimiento
 - Versátil
 - Standard soportado



CUÁL ES MI PERÍMETRO?

- Importancia de los conceptos
 - Borde de nuestra red
 - Red Local
 - DMZ

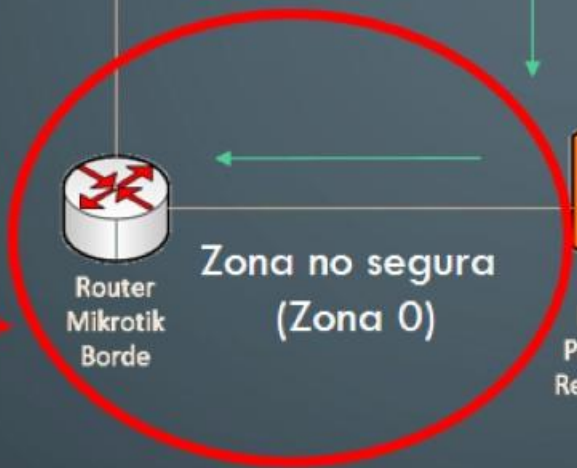


BORDE



Internet

X



Servidor WEB DMZ



Firewall Perímetro Red Interna



Servidores Internos Empresariales



Firewall Perímetro Red Servidores

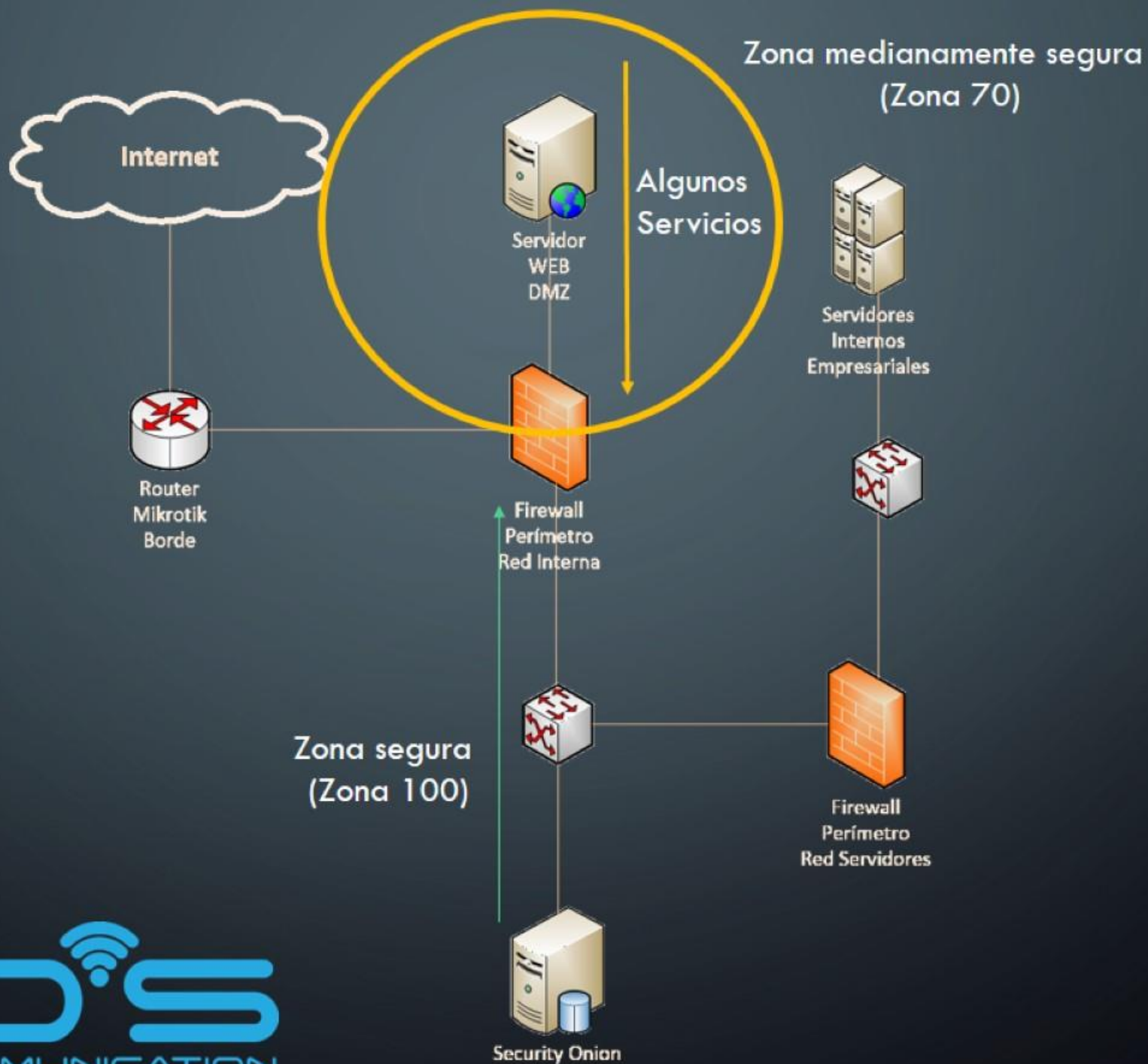


Security Onion

LAN

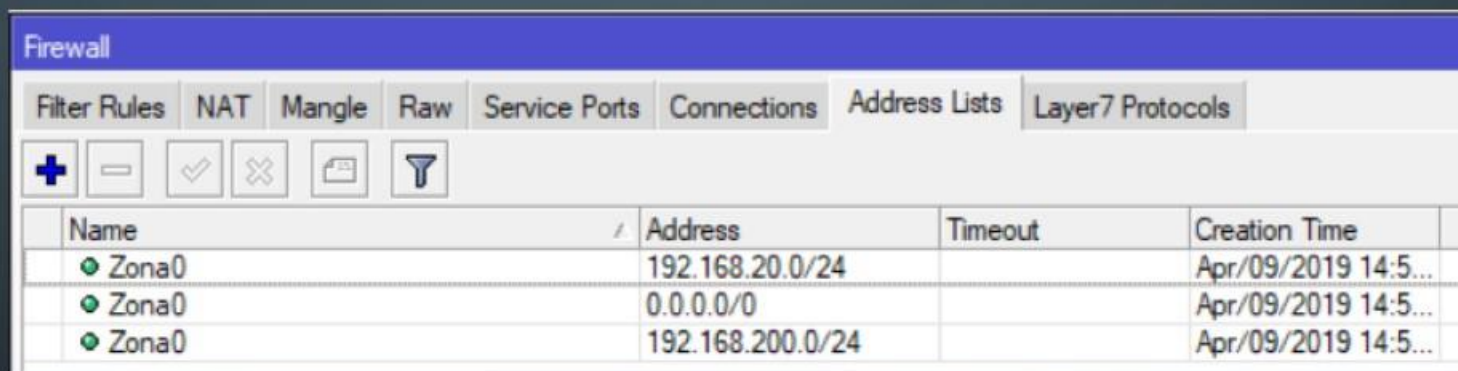


DMZ



FIREWALL BASADO EN ZONAS

- Zona 0 no es segura, se desconfía de todo ese tráfico

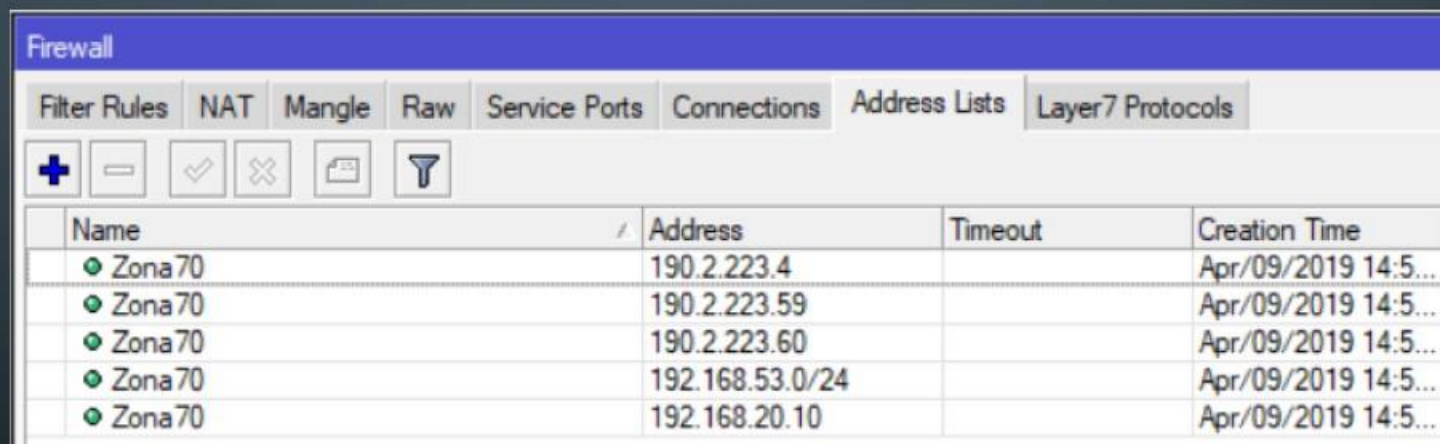


The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Address Lists tab. The window title is "Firewall". Below the title bar are tabs for "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a crossed-out checkmark, a folder, and a funnel. Below the icons is a table with the following columns: Name, Address, Timeout, and Creation Time. The table contains three entries, all named "Zona0".

Name	Address	Timeout	Creation Time
Zona0	192.168.20.0/24		Apr/09/2019 14:5...
Zona0	0.0.0.0/0		Apr/09/2019 14:5...
Zona0	192.168.200.0/24		Apr/09/2019 14:5...

FIREWALL BASADO EN ZONAS, CONT...

- Zona 70 no es tan segura, pero se confía en los servicios necesarios para que la DMZ trabaje correctamente

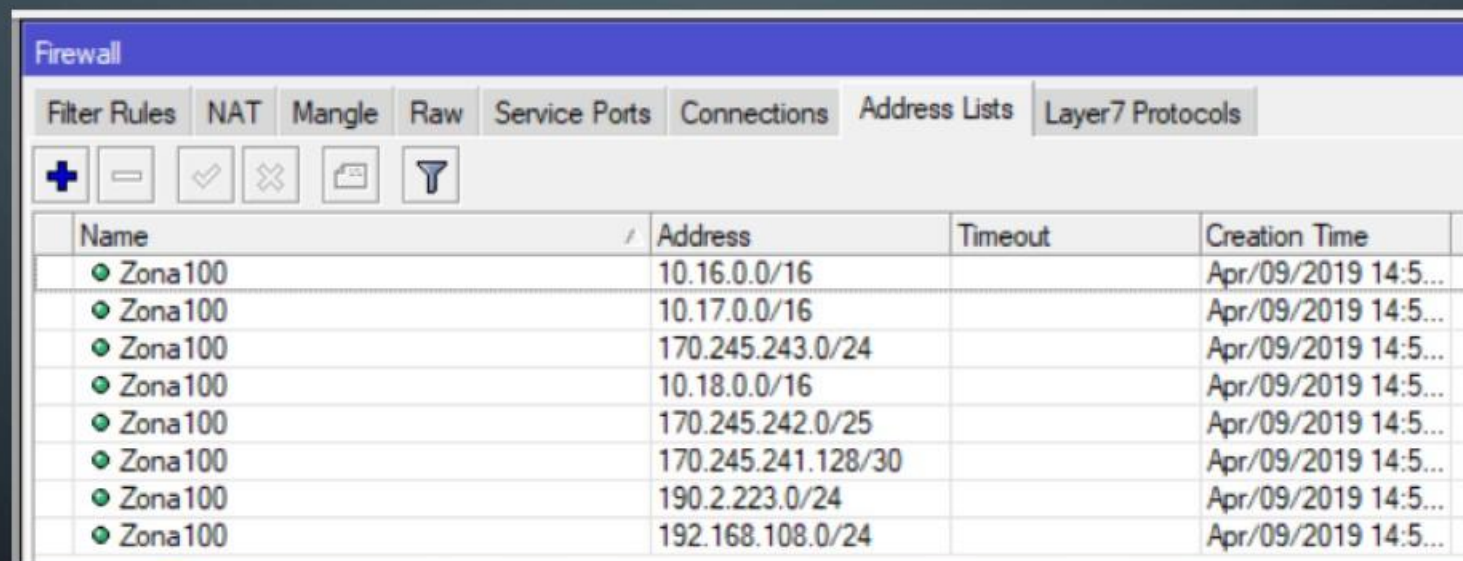


The screenshot shows the Mikrotik WinBox interface for configuring Firewall Address Lists. The 'Address Lists' tab is selected. Below the navigation tabs, there are several icons for adding, deleting, and filtering lists. The main area displays a table with the following data:

Name	Address	Timeout	Creation Time
Zona70	190.2.223.4		Apr/09/2019 14:5...
Zona70	190.2.223.59		Apr/09/2019 14:5...
Zona70	190.2.223.60		Apr/09/2019 14:5...
Zona70	192.168.53.0/24		Apr/09/2019 14:5...
Zona70	192.168.20.10		Apr/09/2019 14:5...

FIREWALL BASADO EN ZONAS, CONT...

- Zona 100, en la cual se confía totalmente



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the 'Address Lists' tab. The window title is 'Firewall'. Below the title bar, there are several tabs: 'Filter Rules', 'NAT', 'Mangle', 'Raw', 'Service Ports', 'Connections', 'Address Lists', and 'Layer7 Protocols'. The 'Address Lists' tab is active. Below the tabs, there are several icons: a plus sign, a minus sign, a checkmark, a cross, a folder, and a funnel. Below the icons is a table with the following columns: 'Name', 'Address', 'Timeout', and 'Creation Time'. The table contains eight rows, all with 'Zona100' in the 'Name' column and various IP address ranges in the 'Address' column. The 'Creation Time' for all entries is 'Apr/09/2019 14:5...'. The 'Timeout' column is empty for all entries.

Name	Address	Timeout	Creation Time
Zona100	10.16.0.0/16		Apr/09/2019 14:5...
Zona100	10.17.0.0/16		Apr/09/2019 14:5...
Zona100	170.245.243.0/24		Apr/09/2019 14:5...
Zona100	10.18.0.0/16		Apr/09/2019 14:5...
Zona100	170.245.242.0/25		Apr/09/2019 14:5...
Zona100	170.245.241.128/30		Apr/09/2019 14:5...
Zona100	190.2.223.0/24		Apr/09/2019 14:5...
Zona100	192.168.108.0/24		Apr/09/2019 14:5...

REGLAS APLICADAS

- La aplicación es en la cadena de forward

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
::: Permitir acceso al router red administrativa															
0	✓ acc...	input										adminis...		35.0 KiB	260
::: Permitir conexiones establecidas y relativas (StateFull) de entrada al router															
1	✓ acc...	input												2246.4 KiB	48 008
::: Denegar acceso al router desde cualquier red que no sea la administrativa															
2	✗ drop	input										!admini...		1030.1 KiB	5 112
::: Permitir de Zona 100 a Zona 0															
3	✓ acc...	forward										Zona100	Zona0	1406.9 MiB	6 114 710
::: Permitir de Zona 100 a Zona 70 (DMZ)															
4	✓ acc...	forward										Zona100	Zona70	0 B	0
::: Permitir de Zona 70 (DMZ) a Zona 0															
5	✓ acc...	forward										Zona70	Zona0	0 B	0
::: Denegar de Zona 0 a Zona 100															
6	✗ drop	forward										Zona0	Zona100	63.2 MiB	331 357
::: Denegar de Zona 70 (DMZ) a Zona 0															
7	✗ drop	forward												30.5 MiB	61 246

DÓNDE INSPECCIONAR EL TRÁFICO?

- Cada segmento de red es una capa



PUNTOS DE ACCESO

- Problema de seguridad que debe ser manejado correctamente



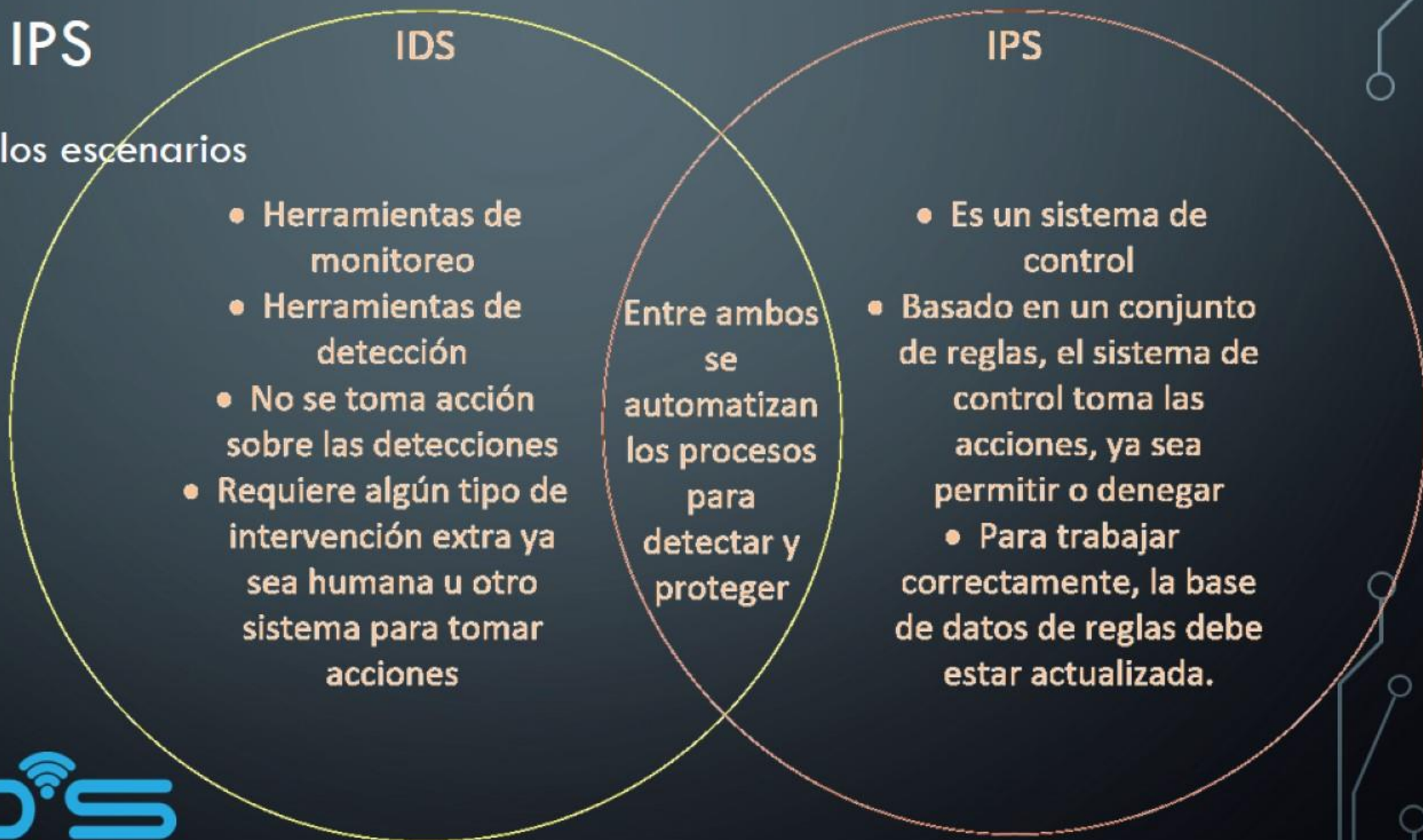
MARCO JURÍDICO

- No bastan las buenas intenciones
- Actuar bajo la legislación



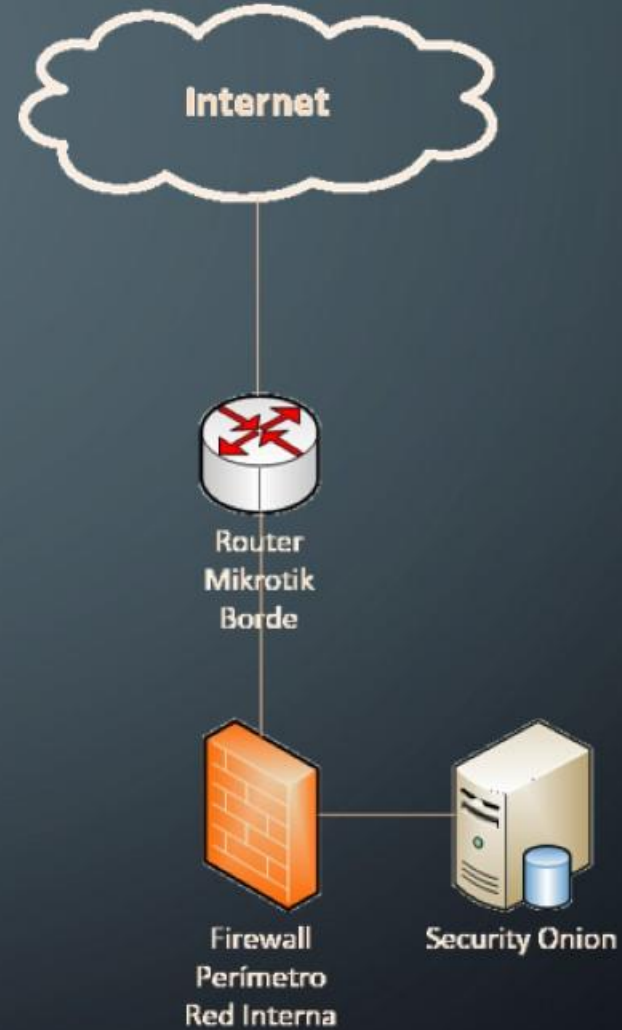
IDS VS IPS

- Aclarando los escenarios



ESTRATEGIA DE ANÁLISIS

- Aspectos a tomar en cuenta
 - Qué impacto tendrá una falla en el sistema?
 - Deseo detectar o también controlar?
 - Deseo inspeccionar profundamente el tráfico?
 - A mayor cantidad de reglas, mayor procesamiento
 - Presupuesto y administración



EN LÍNEA

- Permite el análisis de todo el tráfico pues el mismo pasa a través del Firewall
- Permite análisis de https, ssl o tls, si se cuenta con el certificado de cifrado
- Permite el uso tanto de IPS como de IDS, acorde a las políticas empresariales
- Es único punto de fallo, hay que tenerlo muy en cuenta y mitigarlo/asumirlo
- Hace necesario alto rendimiento y recursos de hardware



El análisis, gestión y control se hacen acá



Router
Mikrotik
Borde

Todo pasa por éste punto



Firewall
Perímetro
Red Interna



Security Onion

FUERA DE LÍNEA

- El tráfico no pasa por el punto de análisis
- El tráfico cifrado no es inspeccionable
- Menor nivel de inspección
- Solo permite monitoreo, no acción (IDS)
- Una falla en el sistema IDS no afecta al tráfico



Internet



Router
Mikrotik
Borde



Security Onion



Intervención
Humana



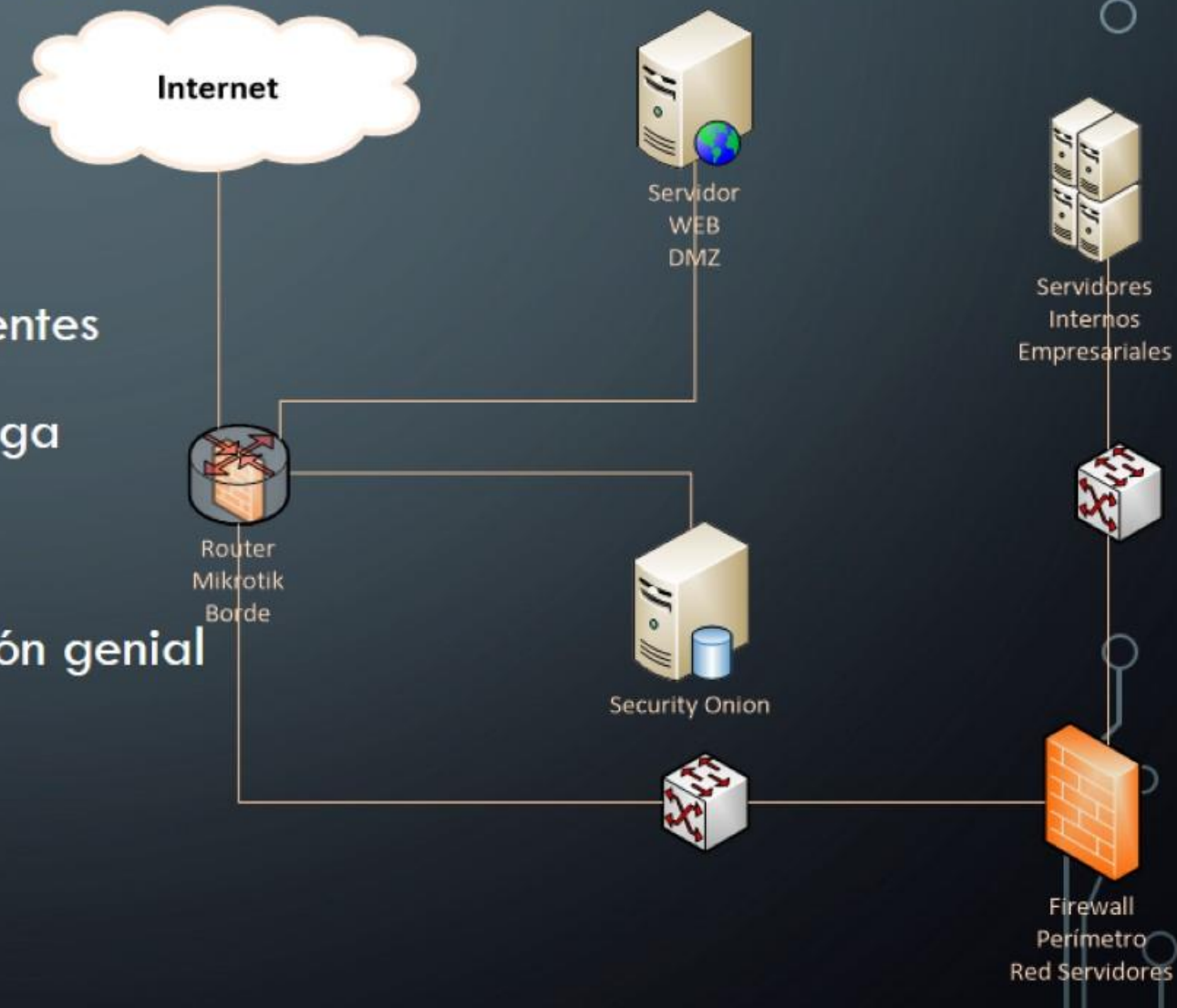
Firewall
Perímetro
Red Interna

El tráfico se recolecta acá



EL ECOSISTEMA DE LA SOLUCIÓN

- Mikrotik hace versátil en análisis en línea
- IPS/IDS – Colector son equipos independientes
- Security Onion analiza el tráfico que le llega
- Security Onion toma las decisiones
- Mikrotik como Firewall y Router, combinación genial



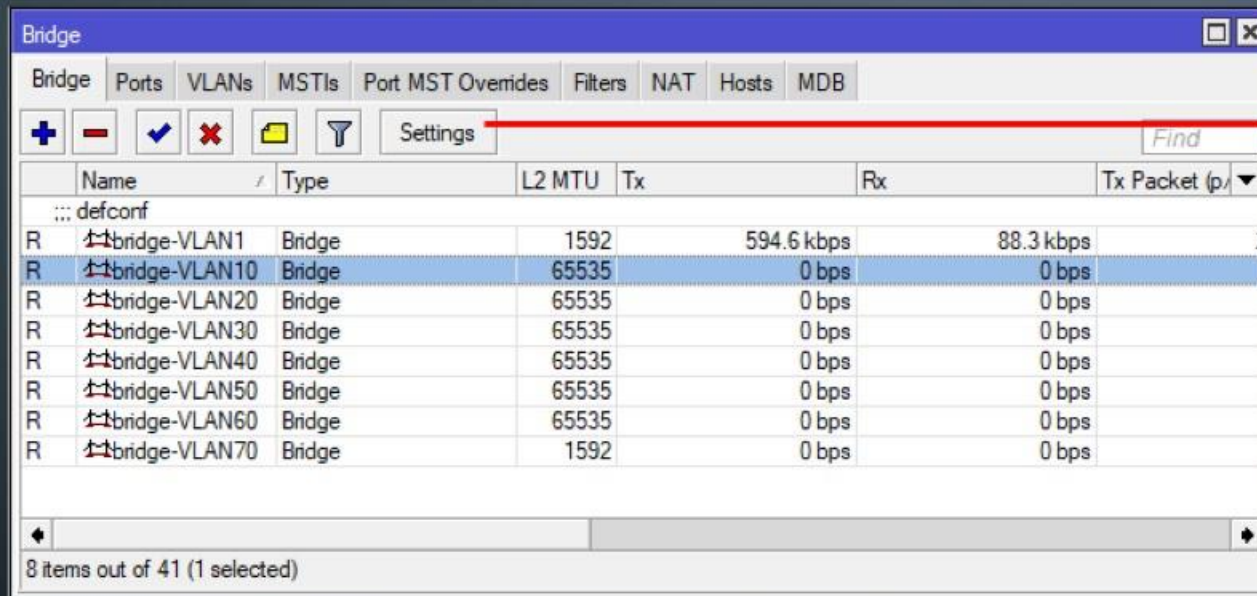
MIKROTIK, EL COLECTOR DE DATOS

- Puntos clave:
 - Definir correctamente la capa 2
 - Definir correctamente la capa 3
 - Definir correctamente el tráfico entre subredes
 - Definir correctamente en esquema NAT/DNAT

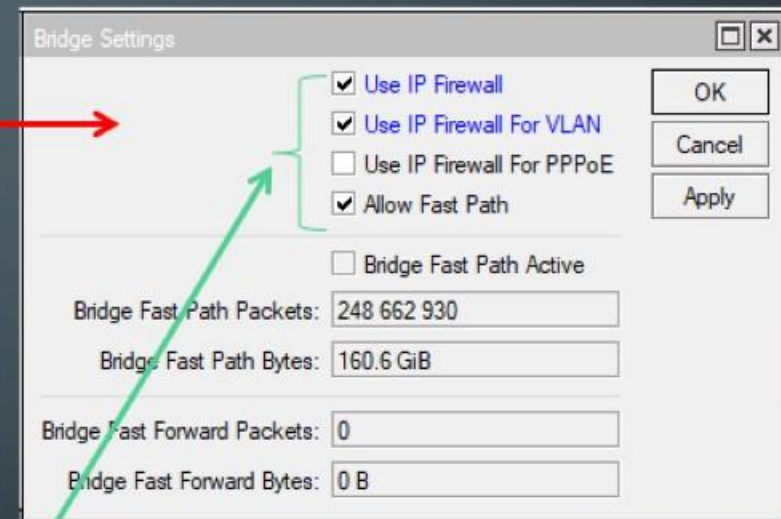
CONFIGURAR EL MIKROTIK

- Aspectos básicos
 - Estructura de VLAN
 - Subneting correcto
 - Análisis de tráfico en la red
 - Qué comportamiento esperar?

CONFIGURACIONES EN CAPA 2



Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)
bridge-VLAN1	Bridge	1592	594.6 kbps	88.3 kbps	
bridge-VLAN10	Bridge	65535	0 bps	0 bps	
bridge-VLAN20	Bridge	65535	0 bps	0 bps	
bridge-VLAN30	Bridge	65535	0 bps	0 bps	
bridge-VLAN40	Bridge	65535	0 bps	0 bps	
bridge-VLAN50	Bridge	65535	0 bps	0 bps	
bridge-VLAN60	Bridge	65535	0 bps	0 bps	
bridge-VLAN70	Bridge	1592	0 bps	0 bps	



Bridge Settings

- Use IP Firewall
- Use IP Firewall For VLAN
- Use IP Firewall For PPPoE
- Allow Fast Path
- Bridge Fast Path Active

Bridge Fast Path Packets: 248 662 930

Bridge Fast Path Bytes: 160.6 GiB

Bridge Fast Forward Packets: 0

Bridge Fast Forward Bytes: 0 B

OK Cancel Apply

Activar estas opciones para manejar el tráfico

CONFIGURACIONES EN CAPA 2, CONT...

- Configuraciones de VLAN, Interfaces virtuales y puertos

Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

+ - ✓ ✗ 📁 🔍 Find

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge-VLAN10	10		
bridge-VLAN10	1		bridge-VLAN10
bridge-VLAN20	20		bridge-VLAN20
bridge-VLAN30	30		bridge-VLAN30
bridge-VLAN40	40		bridge-VLAN40
bridge-VLAN50	50		bridge-VLAN50
bridge-VLAN60	60		bridge-VLAN60
bridge-VLAN70	70		bridge-VLAN70

Interface List

Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE ...

+ - ✓ ✗ 📁 🔍 Find

	Name	Type	MTU	Actual MTU	L2 MTU	Tx
R	VLAN10-GW	VLAN	1500	1500	65531	
R	VLAN20-GW	VLAN	1500	1500	65531	
R	VLAN30-GW	VLAN	1500	1500	65531	
R	VLAN40-GW	VLAN	1500	1500	65531	
R	VLAN50-GW	VLAN	1500	1500	65531	
R	VLAN60-GW	VLAN	1500	1500	65531	
R	VLAN70-GW	VLAN	1500	1500	1588	

7 items out of 41

Bridge VLAN <20>

Bridge: bridge-VLAN20

VLAN IDs: 20

Tagged: sfp-sfpplus 1

Untagged: ether23
ether24

Current Tagged:

Current Untagged: bridge-VLAN20

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled

CONFIGURACIONES EN CAPA 3

Address List

Address	Network	Interface
10.250.10.1/30	10.250.10.0	bridge-VLAN1
192.168.1.1/24	192.168.1.0	bridge-VLAN1
192.168.20.1/24	192.168.20.0	bridge-VLAN20
192.168.30.1/24	192.168.30.0	bridge-VLAN30
192.168.40.1/24	192.168.40.0	bridge-VLAN40
192.168.50.1/24	192.168.50.0	bridge-VLAN50
192.168.60.1/24	192.168.60.0	bridge-VLAN60
192.168.70.1/24	192.168.70.0	bridge-VLAN70

NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: bridge-VLAN1

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Find all

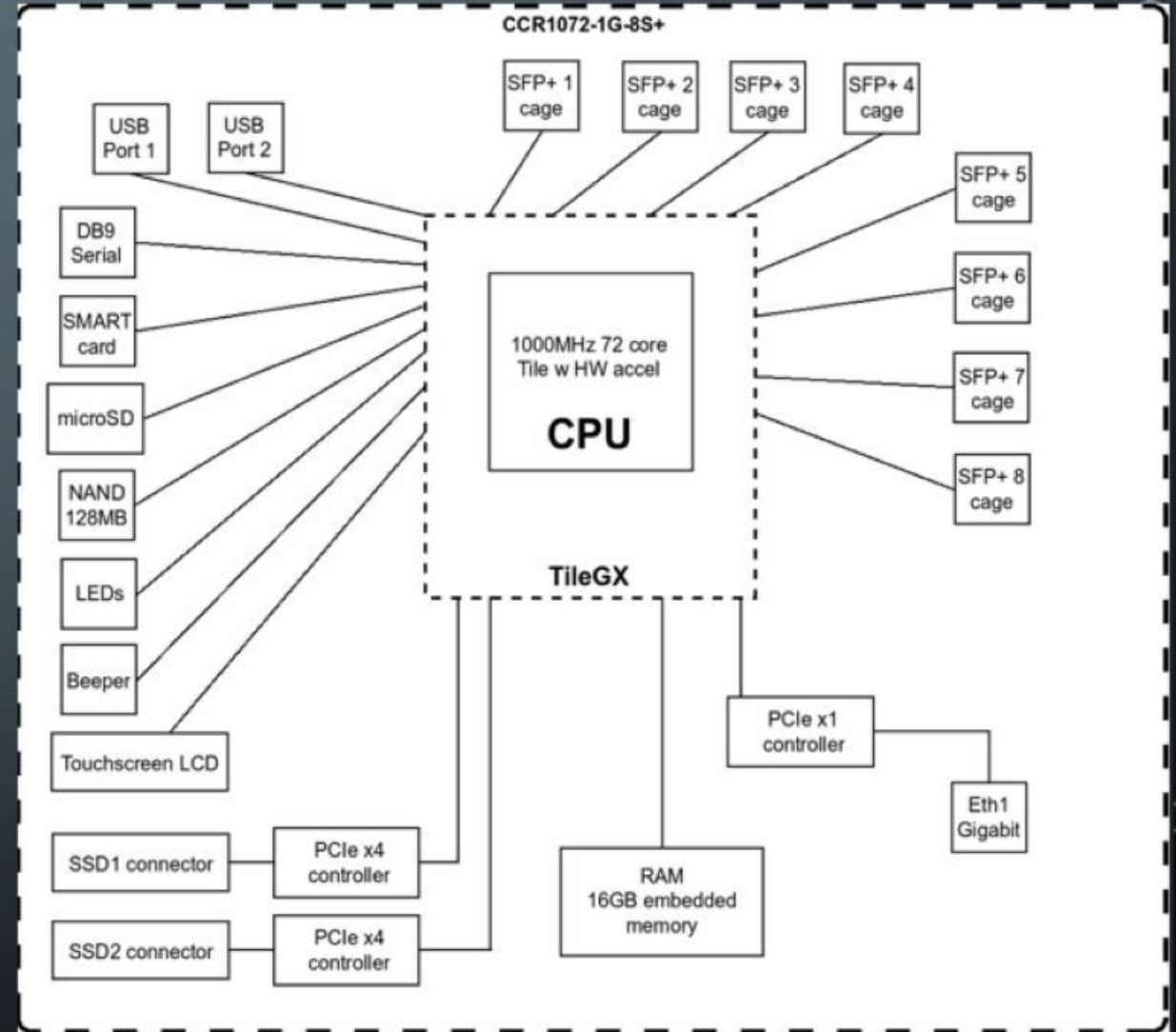
Name	Address	Timeout	Creation Time
RED-SERVIDOR	192.168.1.0/25		Nov/25/2019 09:...
REDES-A-INTERNET	REDES-INTERNAS		Nov/25/2019 09:...
REDES-A-INTERNET	REDES-SUCURSALES		Nov/25/2019 09:...
REDES-A-INTERNET	RED-SERVIDOR		Nov/25/2019 09:...
REDES-INTERNAS	192.168.20.0/24		Nov/25/2019 09:...
REDES-INTERNAS	192.168.30.0/24		Nov/25/2019 09:...
REDES-INTERNAS	192.168.40.0/24		Nov/25/2019 09:...
REDES-INTERNAS	192.168.50.0/24		Nov/25/2019 09:...
REDES-INTERNAS	192.168.60.0/24		Nov/25/2019 09:...
REDES-INTERNAS	192.168.70.0/24		Nov/25/2019 09:...
REDES-SUCURSALES	192.168.1.128/25		Nov/25/2019 09:...
soporte	190.2.223.2-190.2.223.4		Nov/12/2019 09:...
soporte	190.2.223.57-190.2.223.60		Nov/12/2019 09:...
soporte	190.2.217.170		Nov/12/2019 09:...
soporte	192.168.1.0/25		Nov/12/2019 09:...
soporte	10.250.10.0/30		Nov/14/2019 09:...

PORT MIRROR EN MIKROTIK

- Qué es y cómo lo usa Mikrotik (ROS y SwOS)
- Mediante CPU en caso de enrutadores
- Mediante Chip en caso de switches
- Revisar el diagrama de bloques

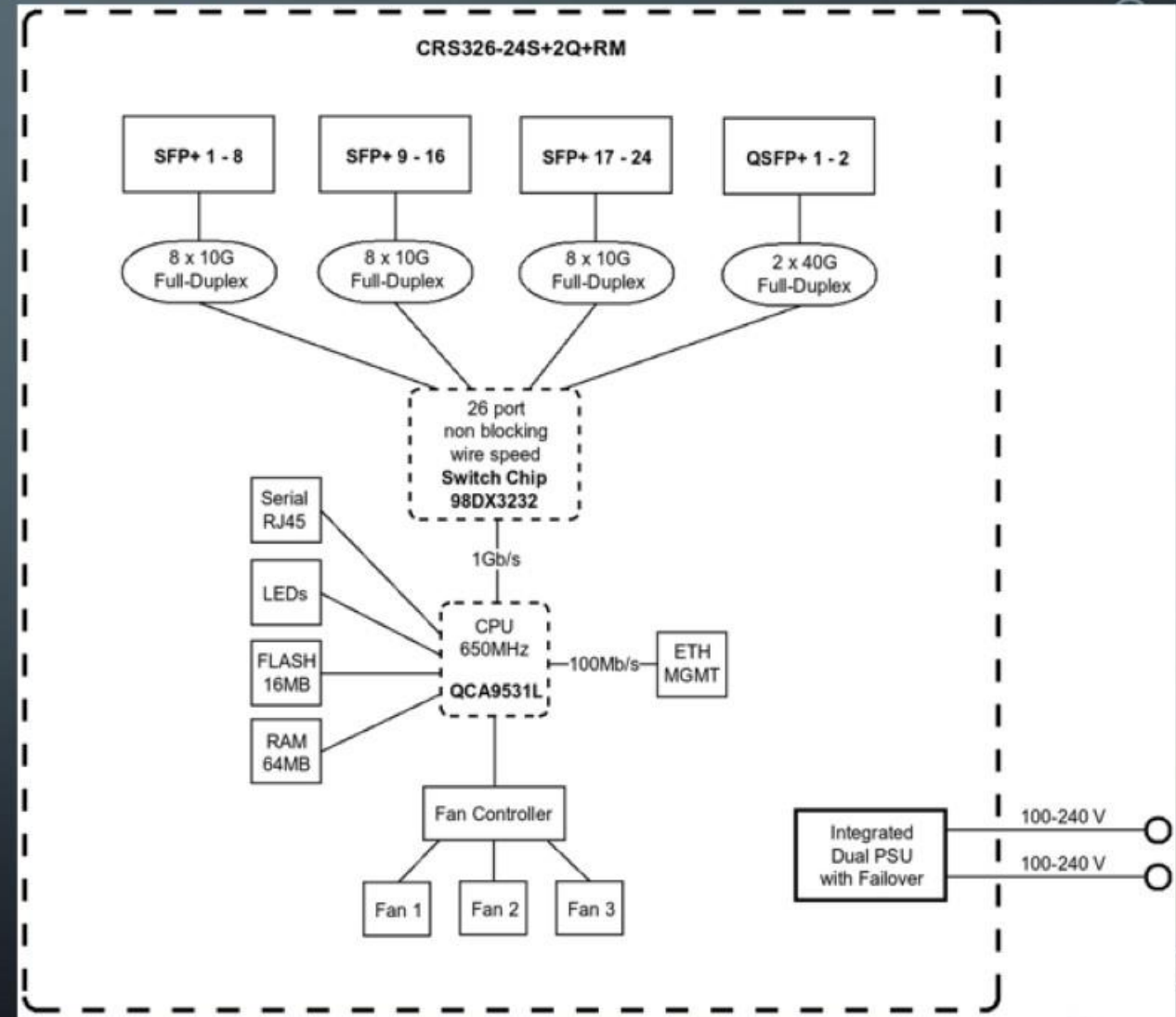
MODELO CCR1072-1G-8S+

- Las funciones de switching (bridge) son asumidas por los CPUs.
- Todo es por software
- Rendimiento no optimizado



MODELO CRS326-24S+2Q+RM

- Chipset especializado
- El CPU maneja el enrutamiento
- El switcheo por hardware
- Rendimiento optimizado

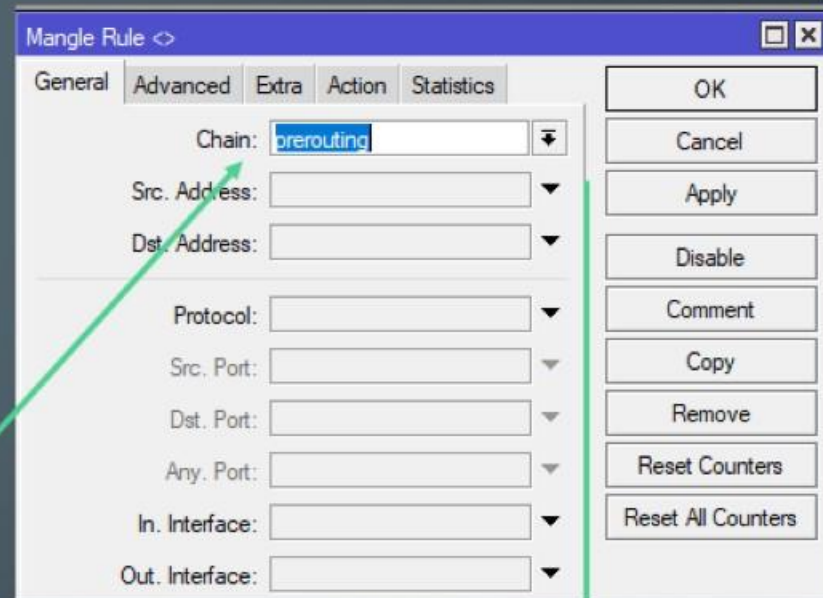


MANGLE

- Se hace por software
- Optimo en routers
- TZSP, protocolo abierto para encapsular otro tráfico mediante UDP



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte
0	sniff TZ...	prerouting						



Mangle Rule <>

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

OK

Cancel

Apply

Disable

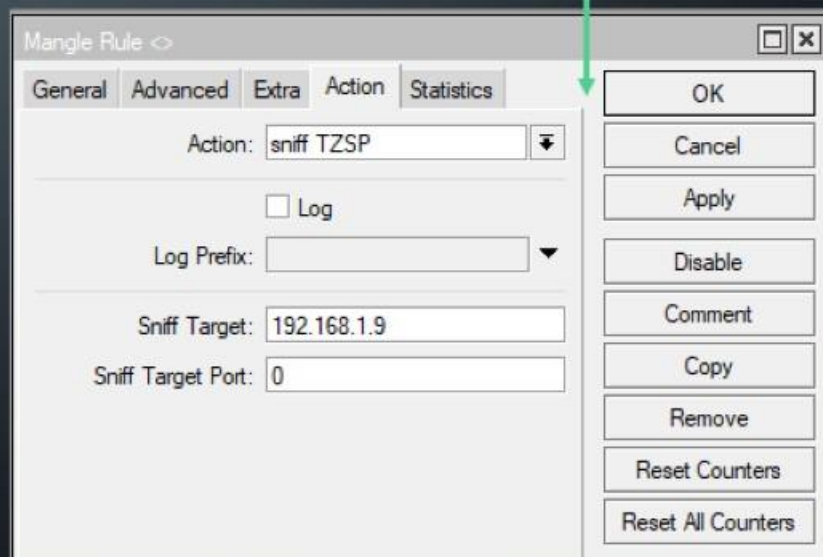
Comment

Copy

Remove

Reset Counters

Reset All Counters



Mangle Rule <>

General Advanced Extra Action Statistics

Action: sniff TZSP

Log

Log Prefix:

Sniff Target: 192.168.1.9

Sniff Target Port: 0

OK

Cancel

Apply

Disable

Comment

Copy

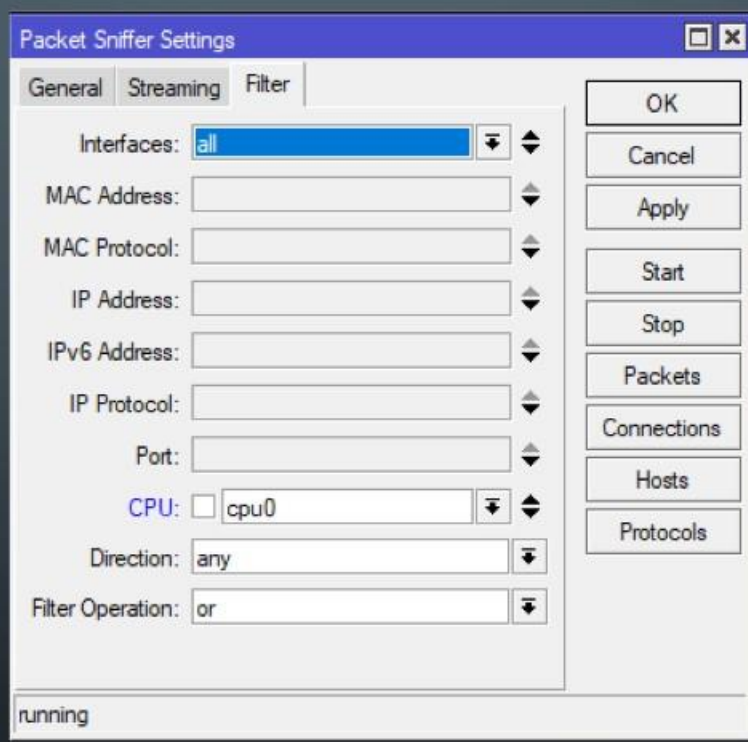
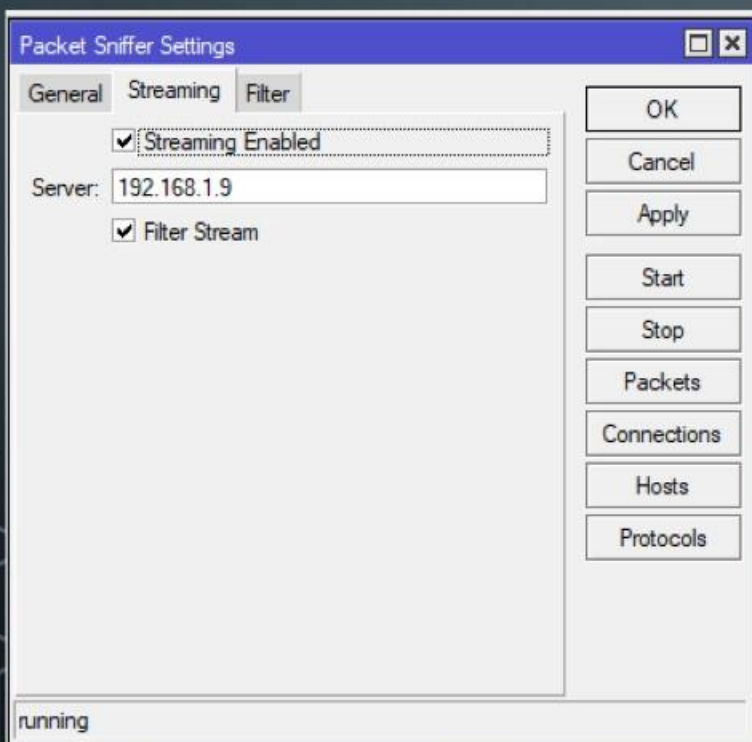
Remove

Reset Counters

Reset All Counters

PACKET SNIFFER

- Ideal en switches
- Flujo de datos continuo (streaming)



Packet Sniffer Connections window showing a table of network connections. The table has columns for Src. Address, Dst. Address, Bytes, Resends, and MSS.

Src. Address	Dst. Address	Bytes	Resends	MSS
10.250.10.1:62522	162.241.142.58:80	0/0	0/0	1460/1460
10.250.10.1:62523	162.241.142.58:80	3136/0	0/0	1460/1460
192.168.1.13:625...	162.241.142.58:80	0/0	0/0	1460/1460
192.168.1.13:625...	162.241.142.58:80	3136/0	3136/0	1460/1460
192.168.1.251:34...	192.168.1.1:8292	6648/86...	6648/21...	0/0
198.178.123.2:72...	10.250.10.1:50813	13824/0	0/0	0/0
198.178.123.2:72...	192.168.1.153:50...	13824/0	0/0	0/0

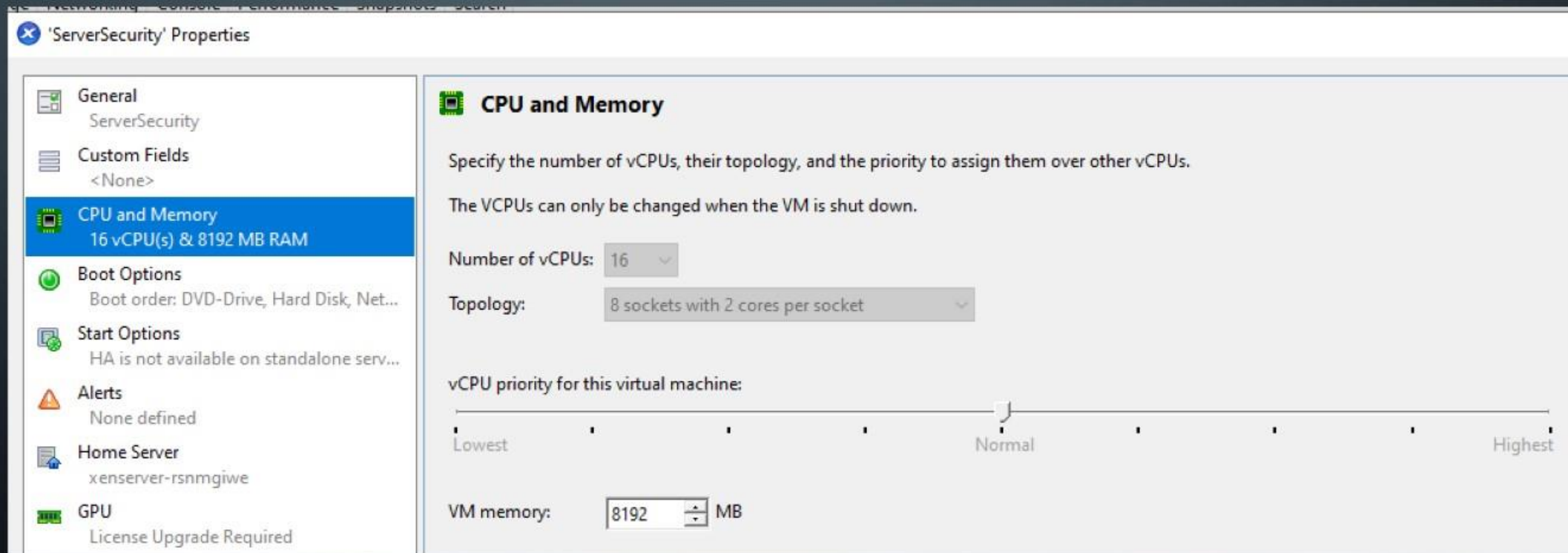
Packet Sniffer Protocols window showing a table of protocol statistics. The table has columns for Protocol, IP Protocol, Port, Packets, Bytes, and Share (%).

Protocol	IP Protocol	Port	Packets	Bytes	Share (%)
4			39	2301	0.23
2048 (ip)			1661	990731	99.42
2048 (ip)	1 (icmp)		3	393	0.03
2048 (ip)	6 (tcp)		1564	959240	96.25
2048 (ip)	17 (udp)		94	31098	3.12
2048 (ip)	6 (tcp)	80	5	282	0.02
2048 (ip)	6 (tcp)	443	40	4900	0.49
2048 (ip)	6 (tcp)	7274	185	108316	10.86
2048 (ip)	6 (tcp)	8292	1334	845742	84.87
2048 (ip)	6 (tcp)	34773	1334	845742	84.87
2048 (ip)	6 (tcp)	40173	3	222	0.02
2048 (ip)	6 (tcp)	40174	3	222	0.02
2048 (ip)	6 (tcp)	47037	1	66	0.00
2048 (ip)	6 (tcp)	49159	5	282	0.02
2048 (ip)	6 (tcp)	50455	3	222	0.02
2048 (ip)	6 (tcp)	50468	3	222	0.02
2048 (ip)	6 (tcp)	50813	185	108316	10.85
2048 (ip)	6 (tcp)	56640	27	3946	0.39
2048 (ip)	17 (udp)	53	45	3330	0.33
2048 (ip)	17 (udp)	67	12	4008	0.40

50 items

SECURITY ONION, EL ANÁLISIS

- Capacidad de procesamiento



The screenshot displays the 'ServerSecurity' Properties dialog box, specifically the 'CPU and Memory' tab. The left sidebar shows various configuration categories, with 'CPU and Memory' selected and highlighted in blue. The main area contains the following settings:

- General:** ServerSecurity
- Custom Fields:** <None>
- CPU and Memory:** 16 vCPU(s) & 8192 MB RAM
- Boot Options:** Boot order: DVD-Drive, Hard Disk, Net...
- Start Options:** HA is not available on standalone serv...
- Alerts:** None defined
- Home Server:** xenserver-rsnmgiwe
- GPU:** License Upgrade Required

CPU and Memory Configuration:

- Number of vCPUs:** 16
- Topology:** 8 sockets with 2 cores per socket
- vCPU priority for this virtual machine:** A slider is positioned at the 'Normal' mark on a scale from 'Lowest' to 'Highest'.
- VM memory:** 8192 MB

COMPONENTES IDS/IPS

- Motor de análisis de tráfico
- Motor de almacenamiento de bitácoras
- Toma de decisiones sobre el tráfico
- Genera los triggers sobre dichas decisiones
- Visualización de eventos



SURICATA/SNORT

INTRUSION
DETECTION

WITH



SURICATA

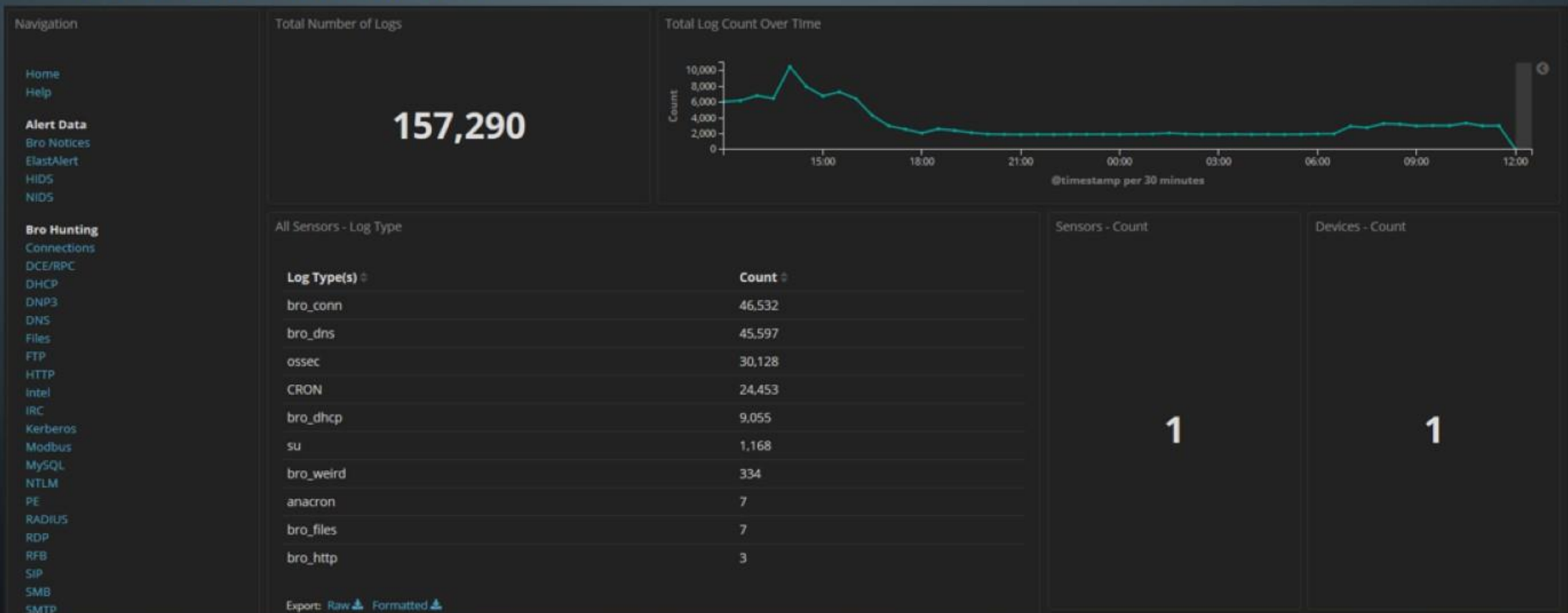


SNORT[®]

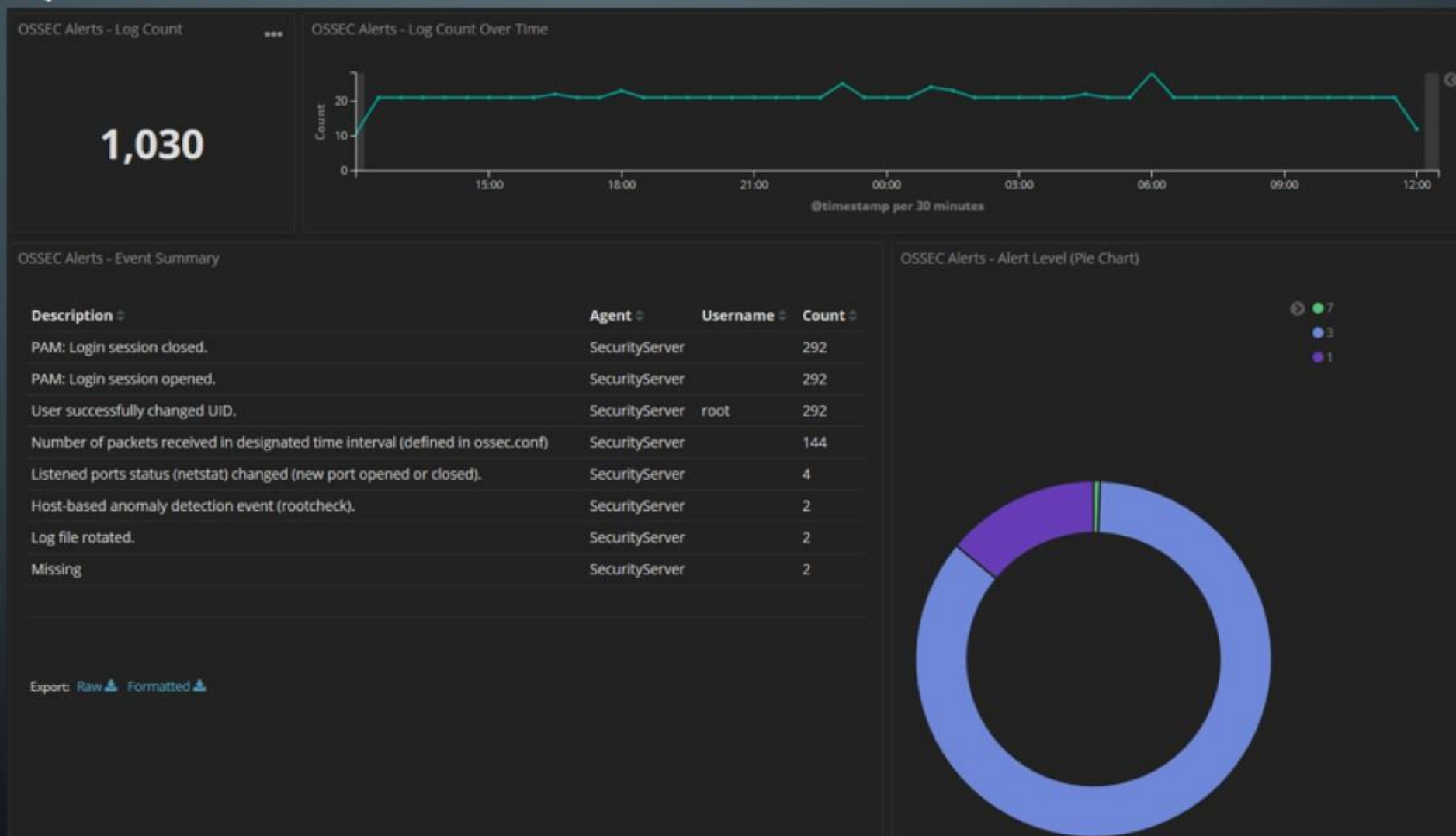
3DS[®]
TELECOMMUNICATION

KIBANA

- Dashboard informativo



KIBANA, CONT...



API MIKROTIK

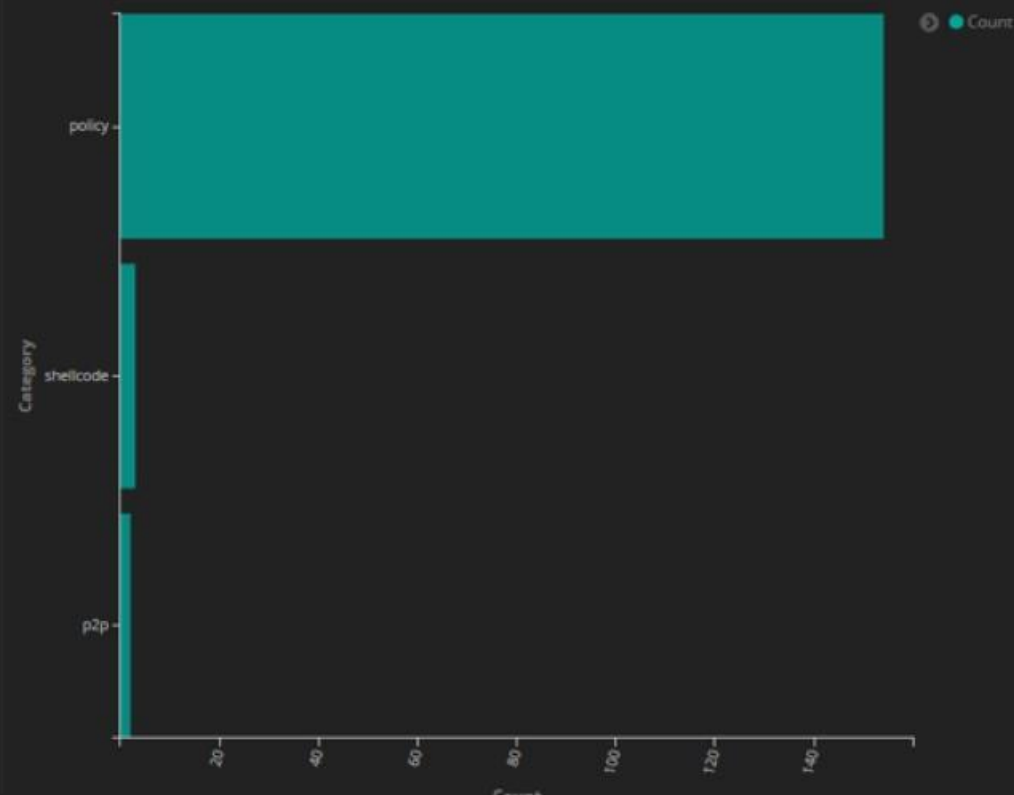
- Transformando nuestro IDS en un IPS
- Permite tomar el flujo de datos y enviarlos al servidor IPS/IDS Security Onion
- Security Onion toma las decisiones acorde a su base de datos de firmas
- Dichas decisiones o triggers se envían al ROS mediante la API para generar los cambios en el firewall necesarios.

EJEMPLO

NIDS - Classification

Classification	Count
Not Suspicious Traffic	154
Executable code was detected	3
Potential Corporate Privacy Violation	2

NIDS Alerts - Category



NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET POLICY Spotify P2P Client	192.168.1.5	192.168.1.255	154
ET SHELLCODE Possible Call with No Offset UDP Shellcode	192.168.1.1	192.168.1.9	3
ET P2P ThunderNetwork UDP Traffic	192.168.1.62	224.0.0.252	2

EJEMPLO, CONT...

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📄 🔍

	Name	Address	Timeout	Creation Time
D	HostBlockedSO	192.168.1.62	00:56:23	Jan/11/2020 12:...
	RED-SERVIDOR	192.168.1.0/25		Nov/25/2019 09:...
	REDES-A-INTERNET	REDES-INTERNAS		Nov/25/2019 09:...

Firewall Rule <>

General Advanced Extra Action Statistics

Src. Address List: HostBlockedSO

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📄 🔍 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	✓ acc...	input										REDE...		0 B	0
1	✓ acc...	input										soporte		1175.5 MiB	11 045 074
2	✓ acc...	input												46.5 MiB	917 810
3	✓ acc...	input			6 (tcp)		8292							2172 B	43
4	✗ drop	input												741.5 MiB	3 567 573
5	✗ drop	forward										HostBl...		0 B	0

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of thin lines that branch out and terminate in small circles, resembling electronic components or nodes on a board. The patterns are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Muchas
GRACIAS