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.

3D'S TELECOMMUNICATION

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.

3D'S TELECOMMUNICATION

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.

3D'S TELECOMMUNICATION

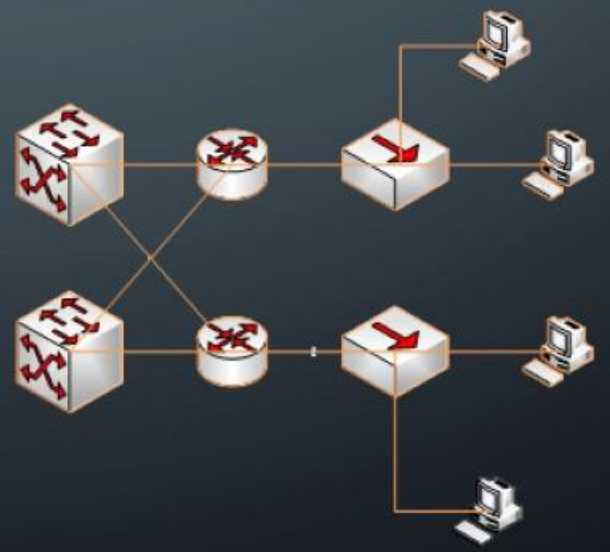
EXPERIENCIA

- 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)

3D'S TELECOMMUNICATION

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.

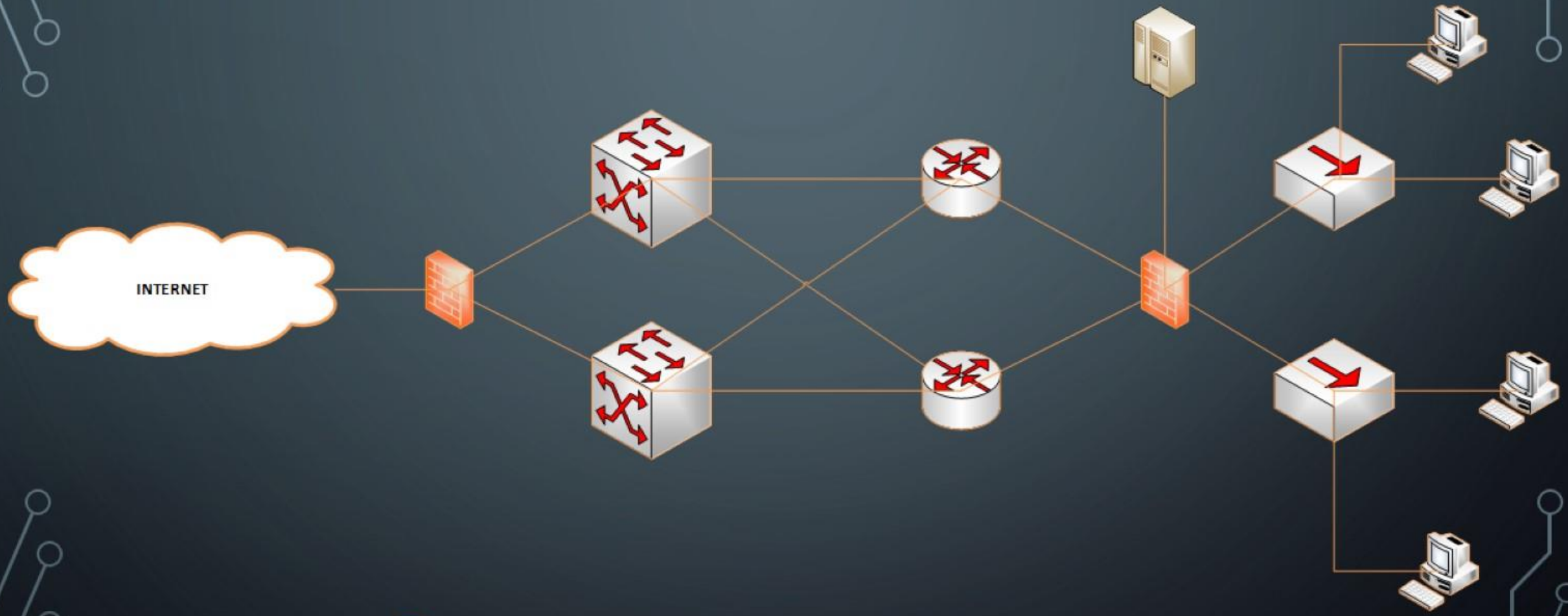


3D'S TELECOMMUNICATION

PROTECCIÓN POR CAPAS

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

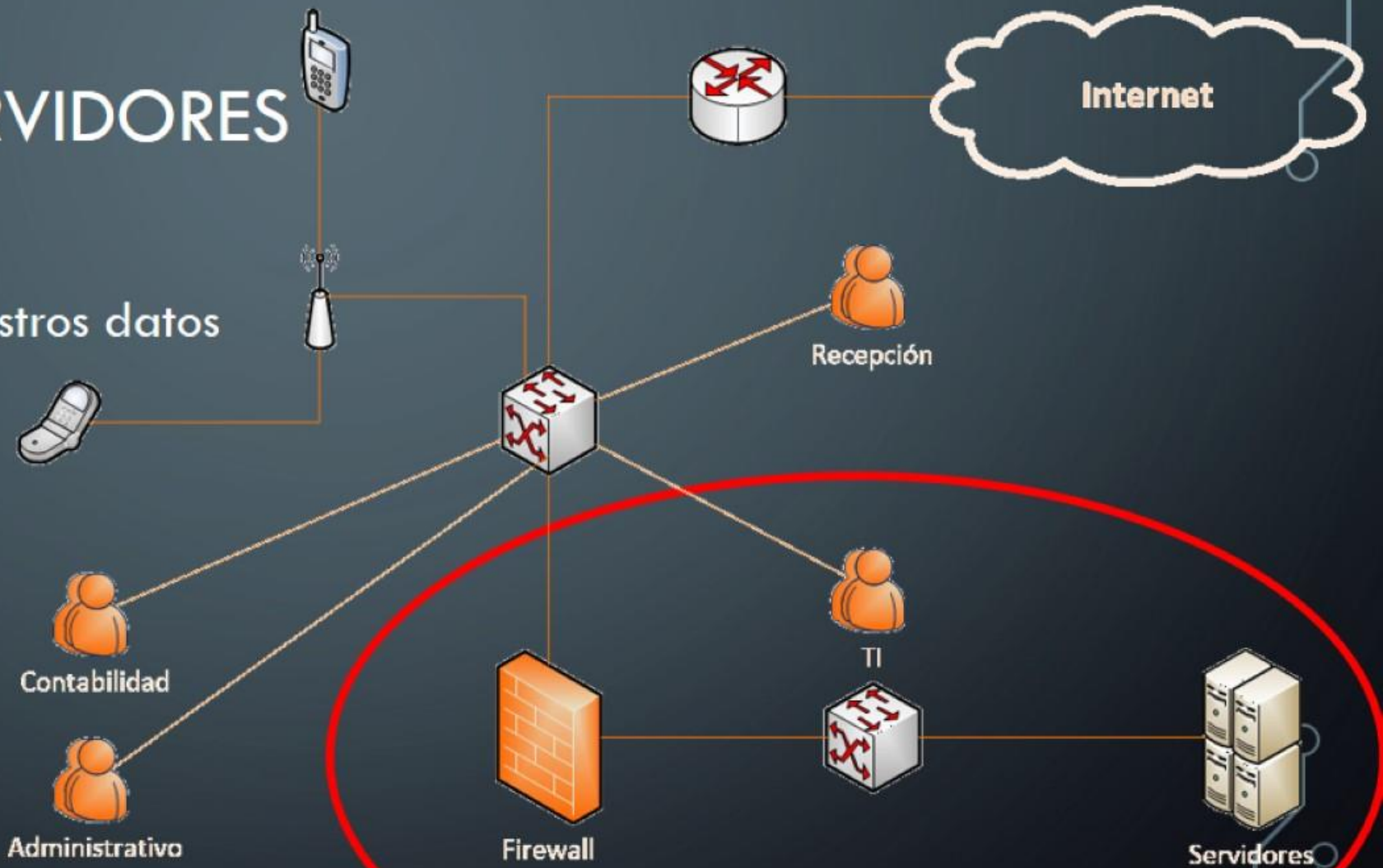
3D'S TELECOMMUNICATION



3D'S TELECOMMUNICATION

SEGURIDAD SERVIDORES

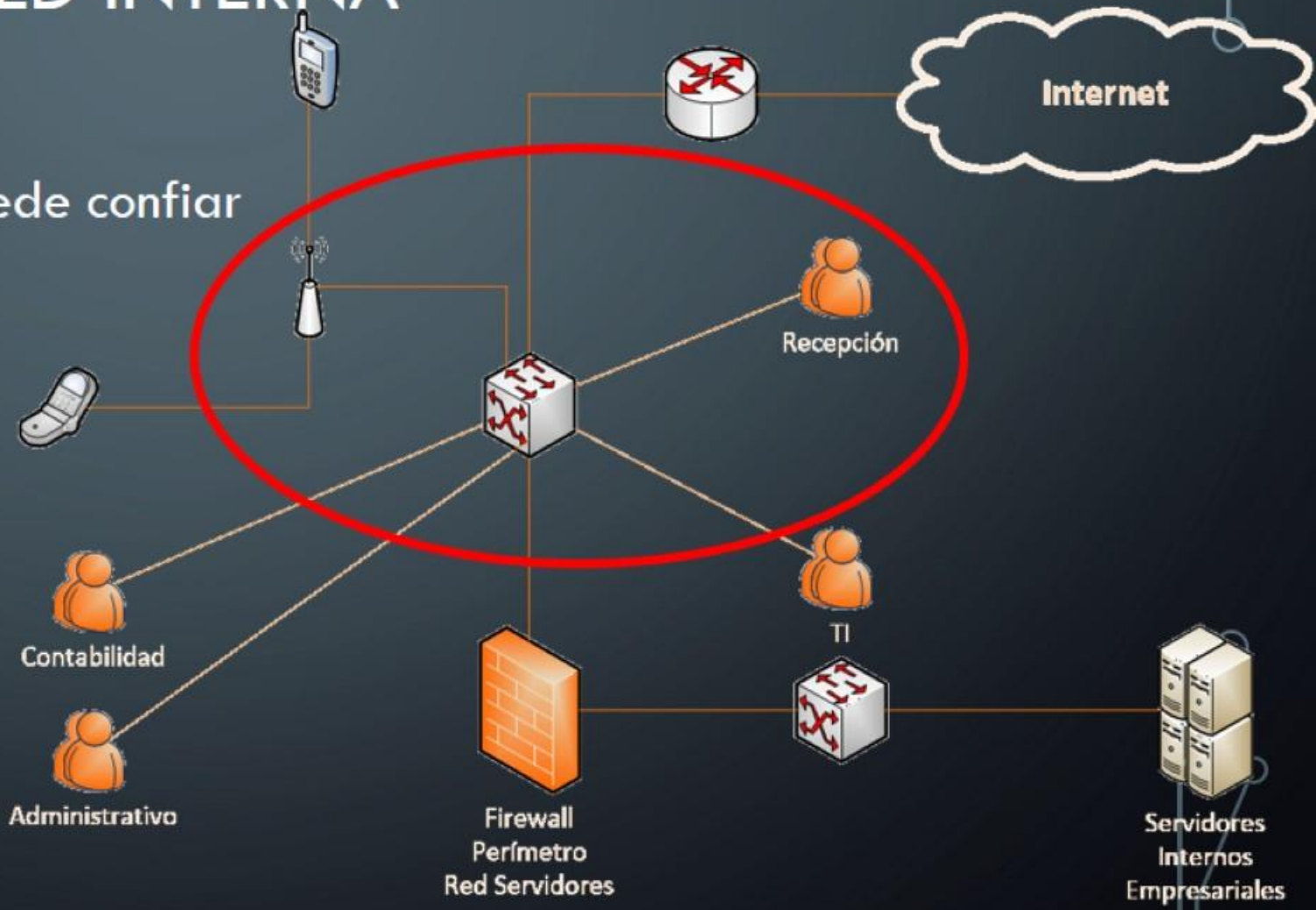
- La importancia de nuestros datos



3D'S TELECOMMUNICATION

SEGURIDAD EN LA RED INTERNA

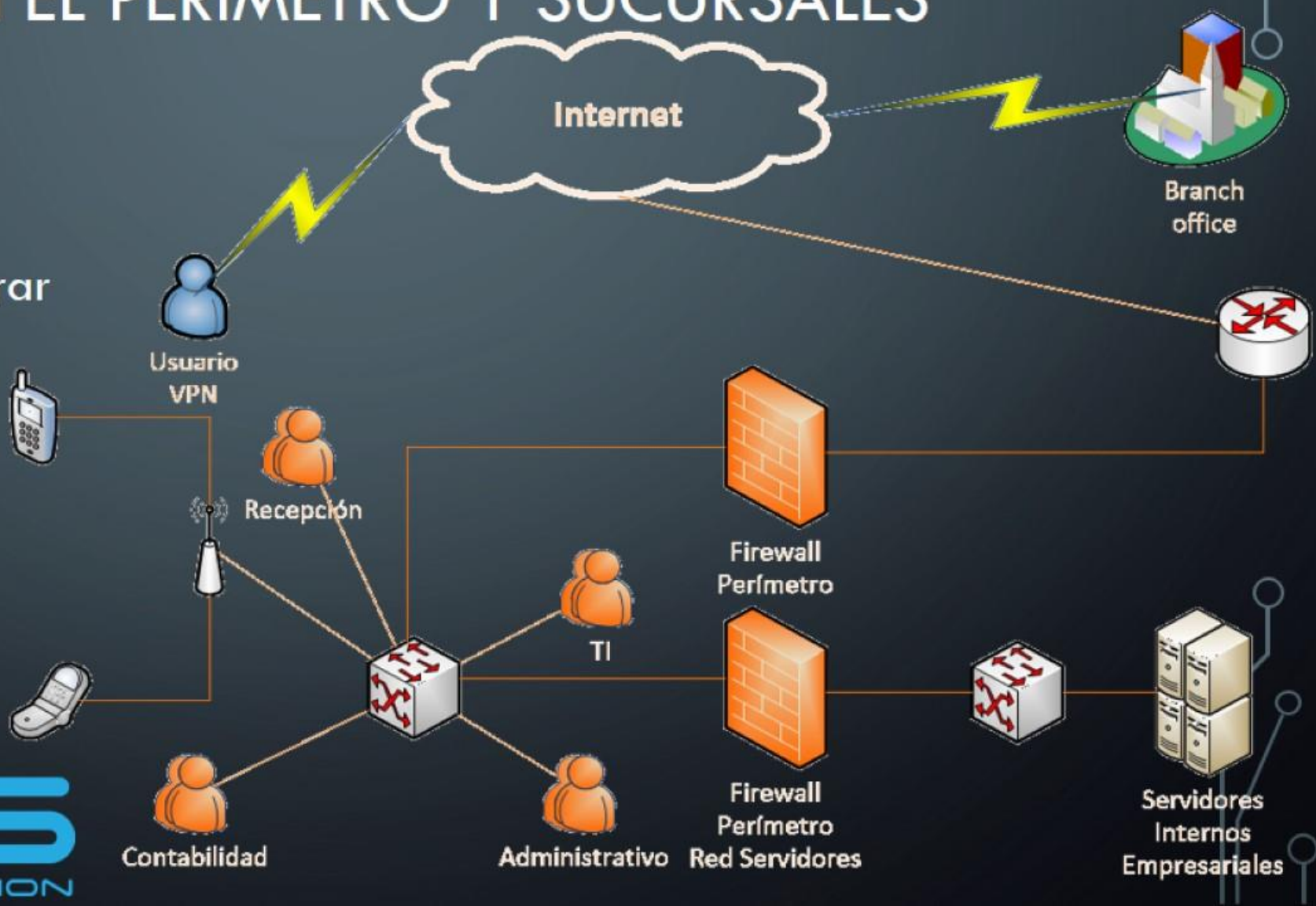
- La confianza donde no se puede confiar



3D'S TELECOMMUNICATION

SEGURIDAD EN EL PERÍMETRO Y SUCURSALES

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



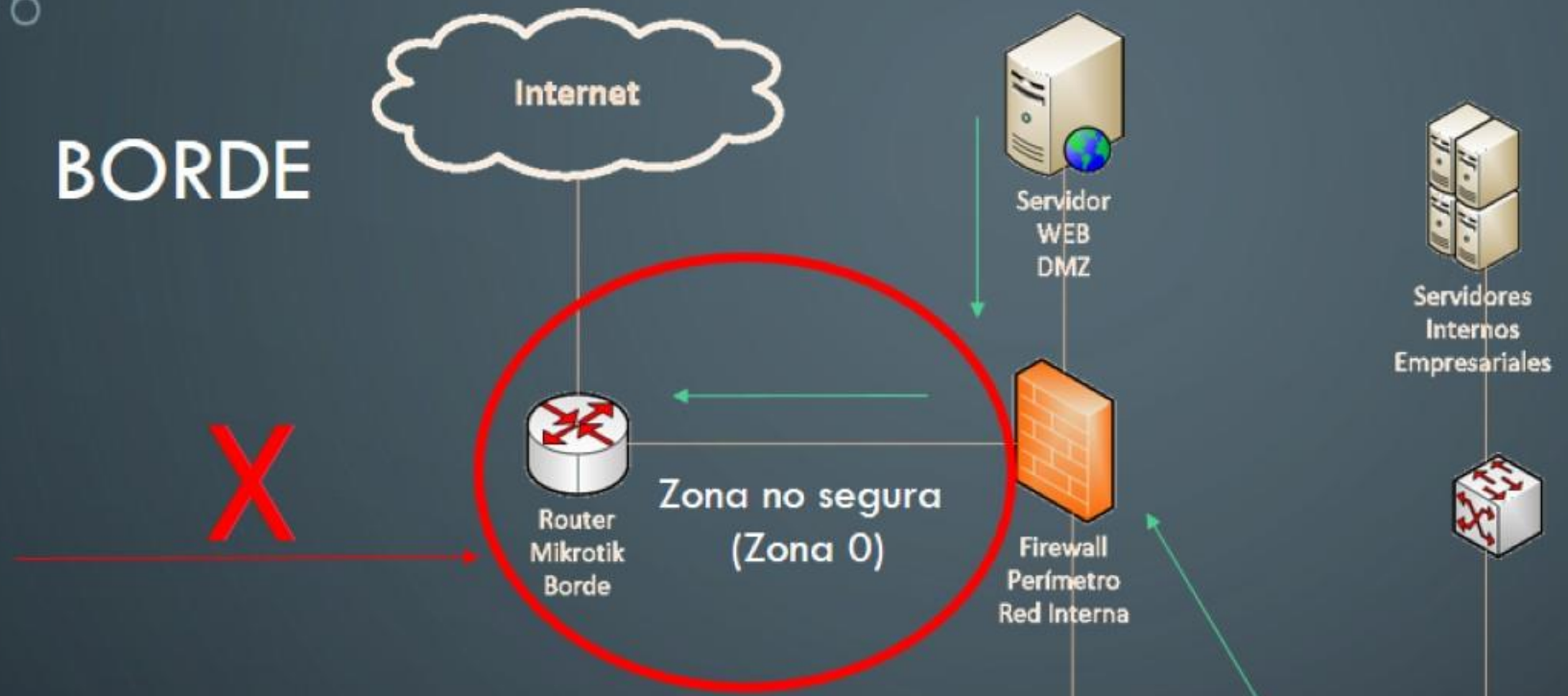
3D'S TELECOMMUNICATION

CUÁL ES MI PERÍMETRO?

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

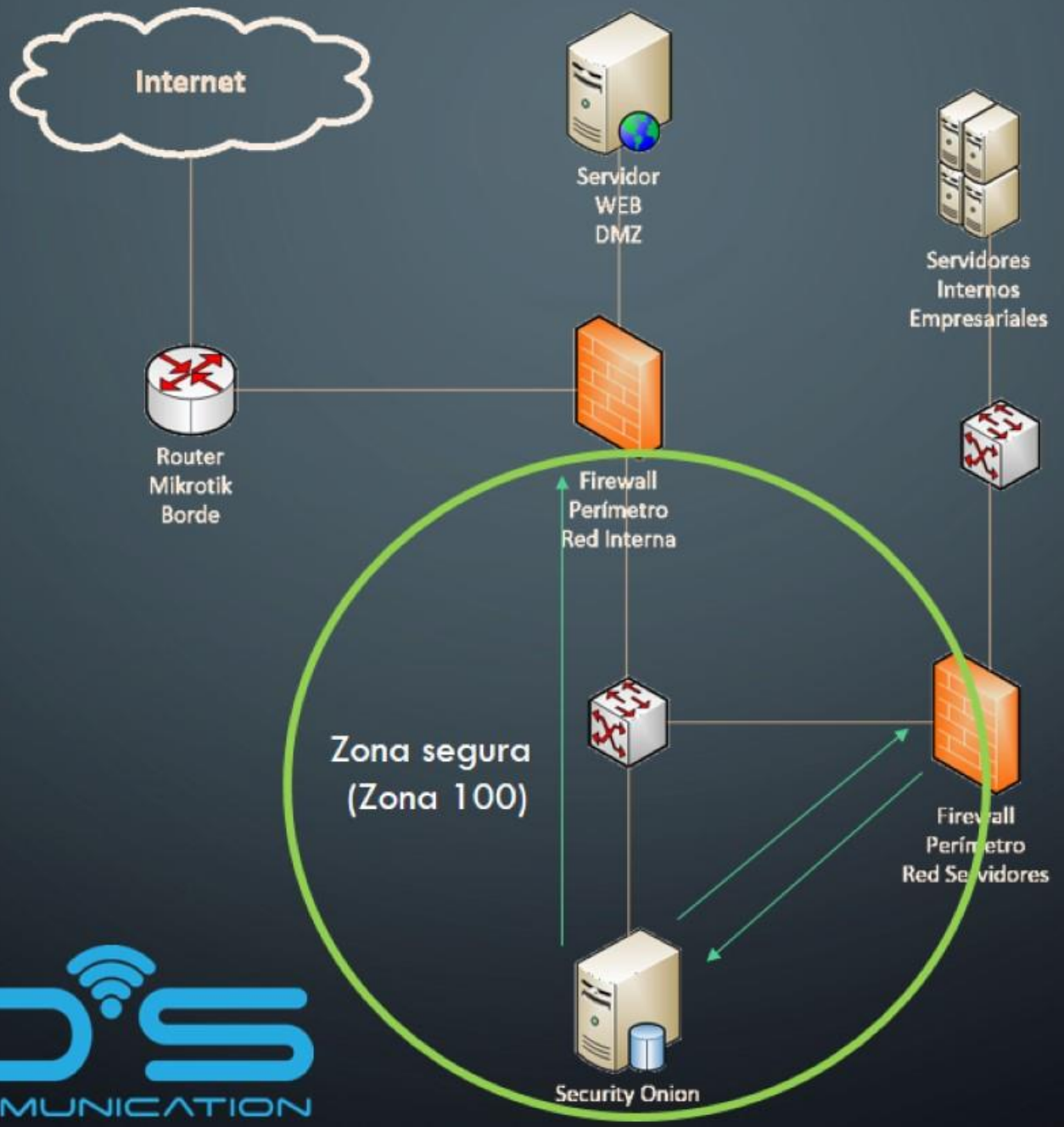
3D'S TELECOMMUNICATION

BORDE



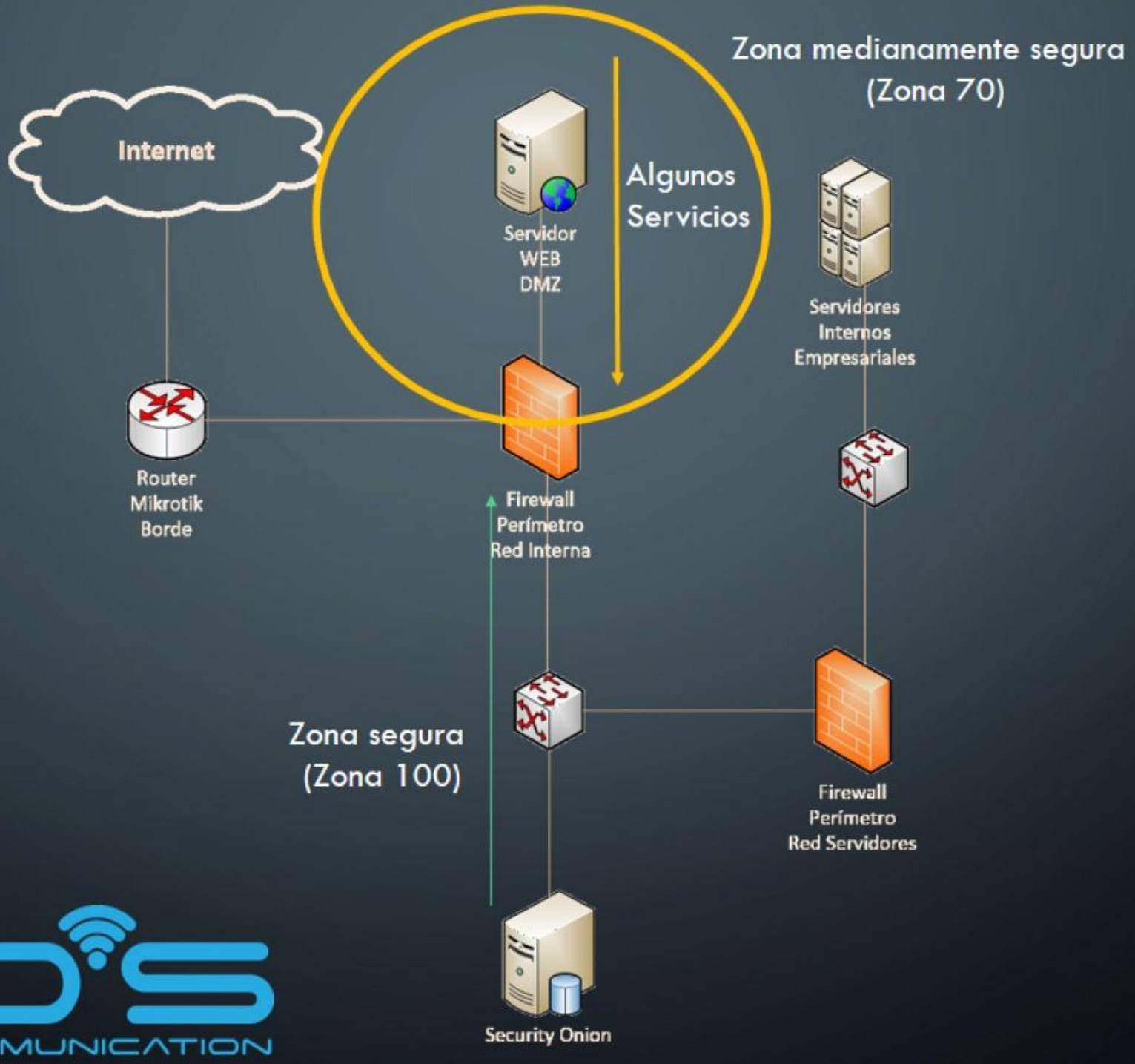
3D'S TELECOMMUNICATION

LAN



3D'S TELECOMMUNICATION

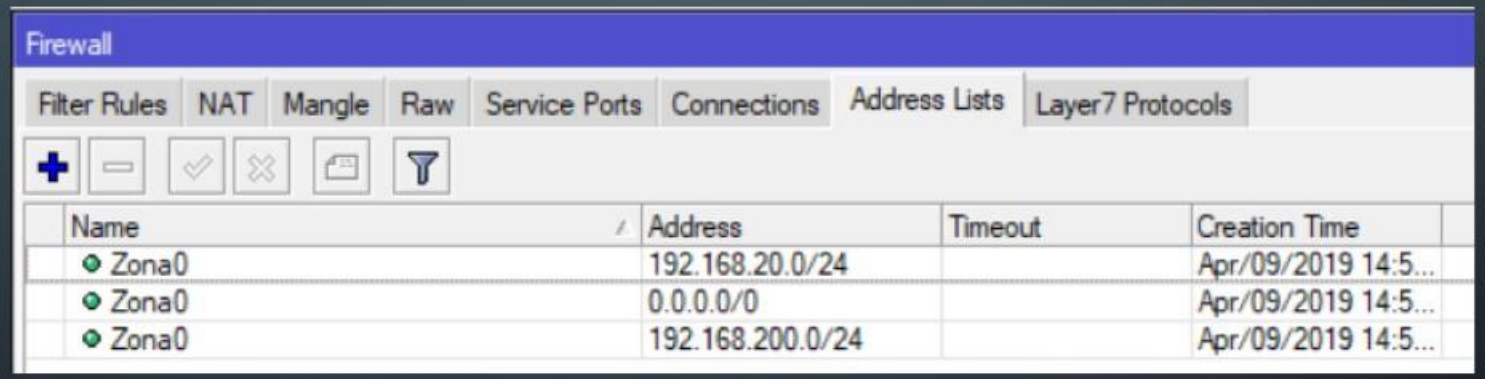
DMZ



3D'S TELECOMMUNICATION

FIREWALL BASADO EN ZONAS

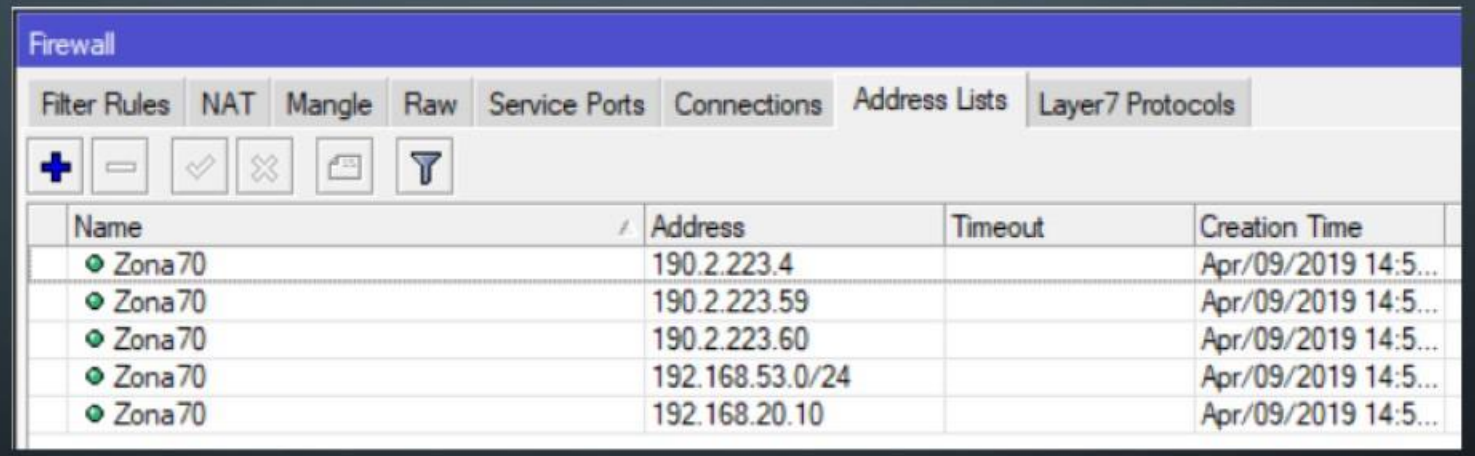
- Zona 0 no es segura, se desconfía de todo ese tráfico



3D'S TELECOMMUNICATION

FIREWALL BASADO EN ZONAS, CONT…

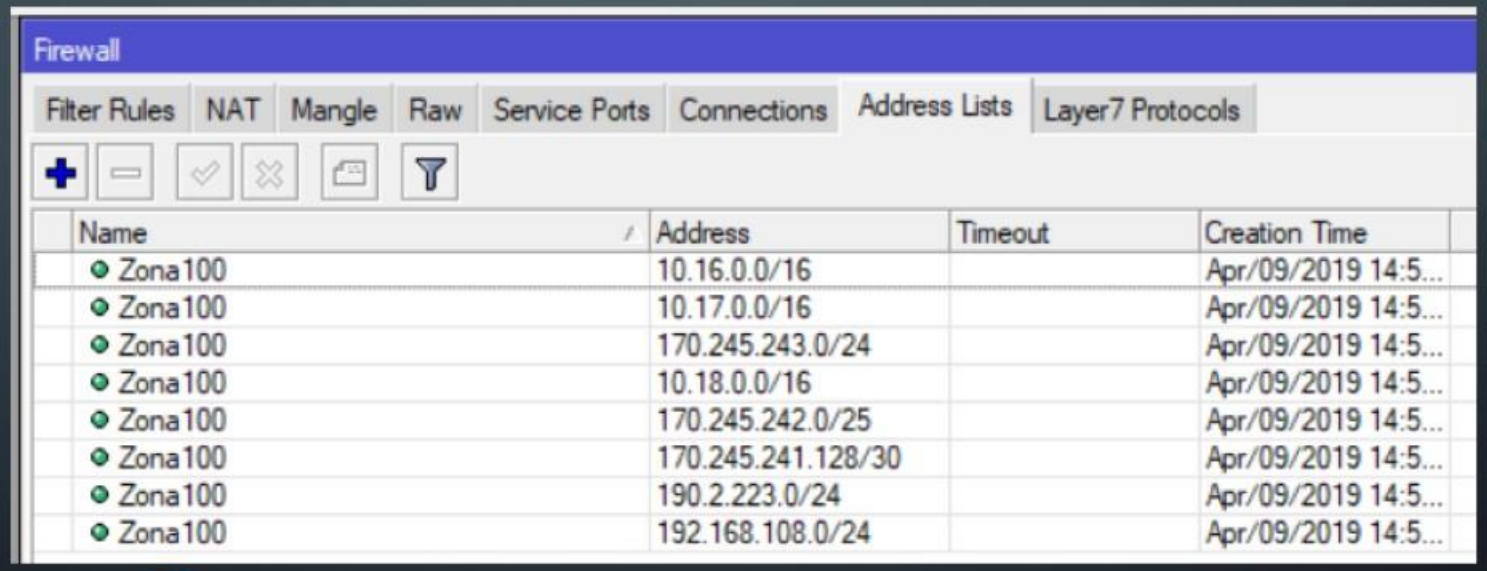
- Zona 70 no es tan segura, pero se confía en los servicios necesarios para que la DMZ trabaje correctamente



3D'S TELECOMMUNICATION

FIREWALL BASADO EN ZONAS, CONT…

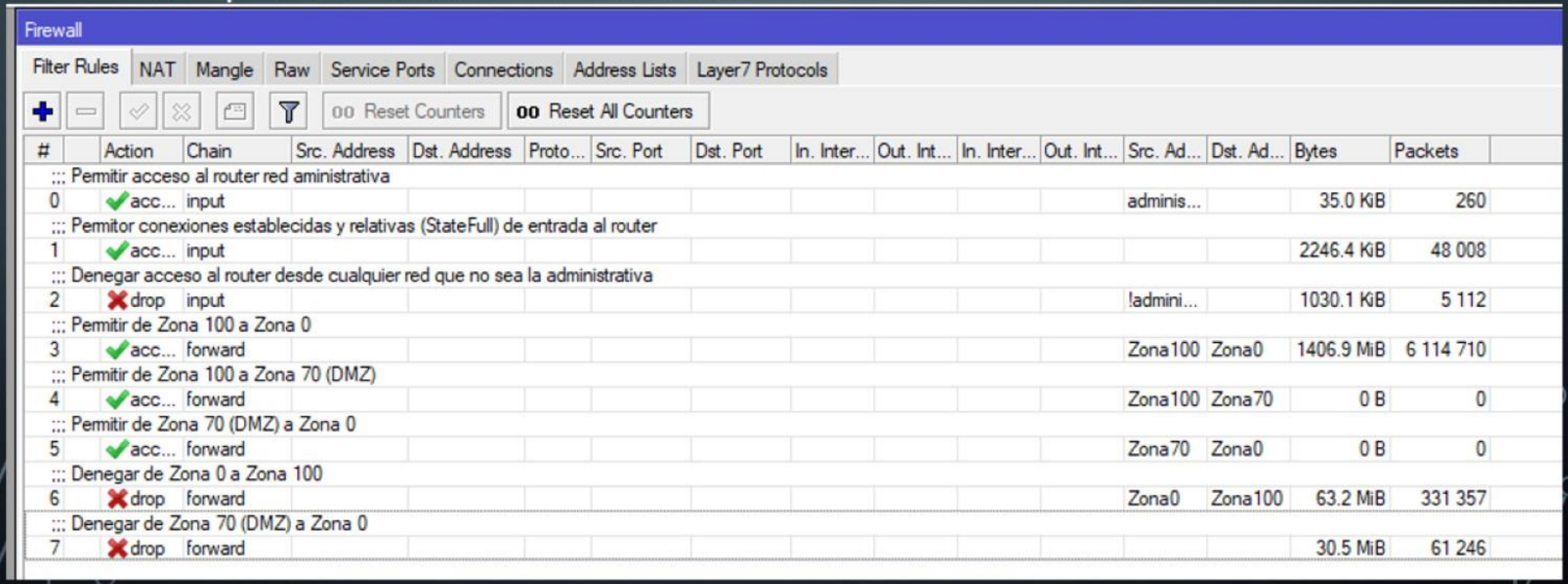
- Zona 100, en la cual se confía totalmente



3D'S TELECOMMUNICATION

REGLAS APLICADAS

- La aplicación es en la cadena de forward



Firewall

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

00 Reset Counters | 00 Reset All Counters

#		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 aministrativa																
0		acc...	input										adminis...		35.0 KiB	260
;;; Permitor 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

3D'S TELECOMMUNICATION

PUNTOS DE ACCESO

- Problema de seguridad que debe ser manejado correctamente

3D'S TELECOMMUNICATION

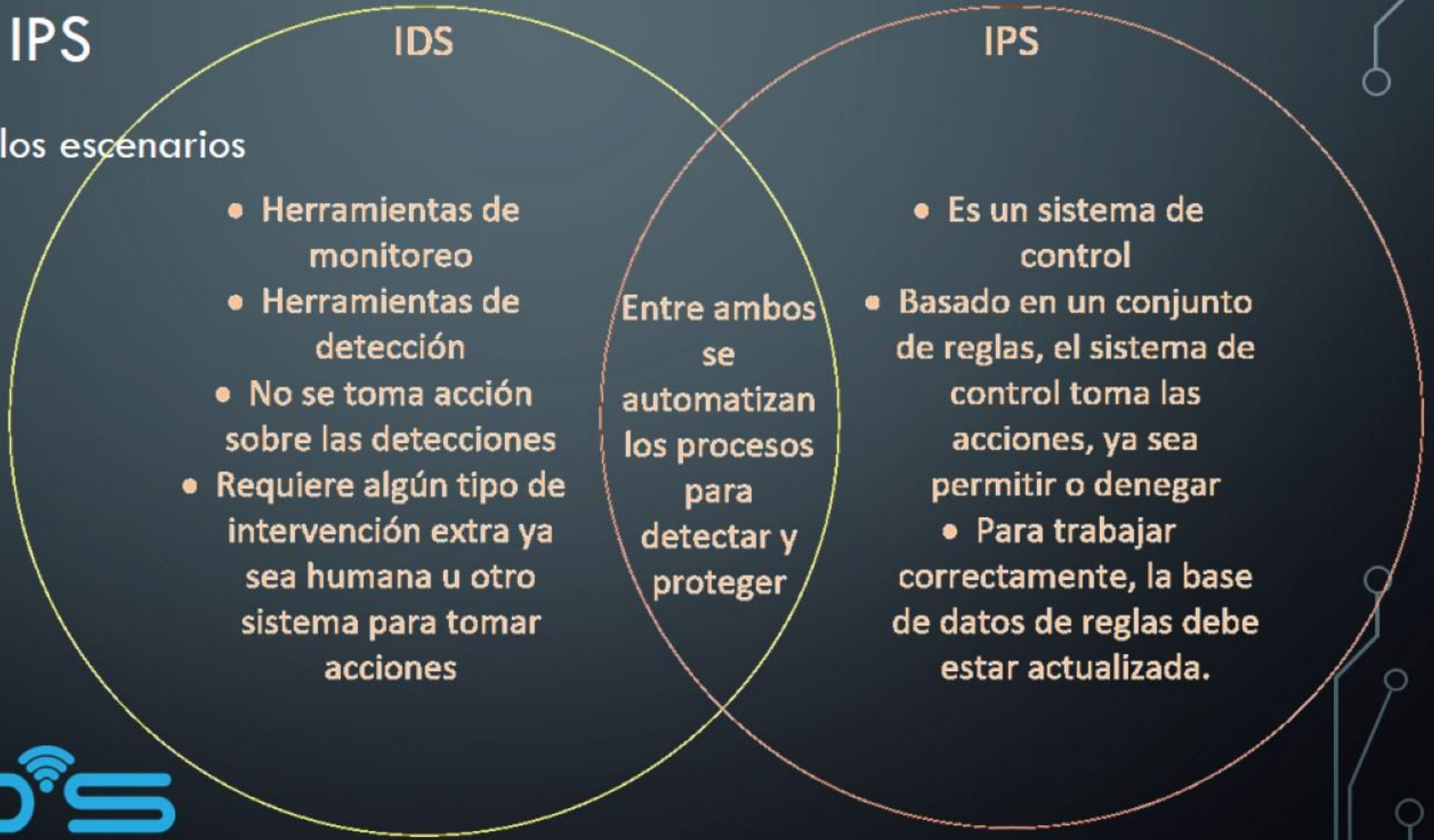
MARCO JURÍDICO

- No bastan las buenas intenciones
- Actuar bajo la legislación

3D'S TELECOMMUNICATION

IDS VS IPS

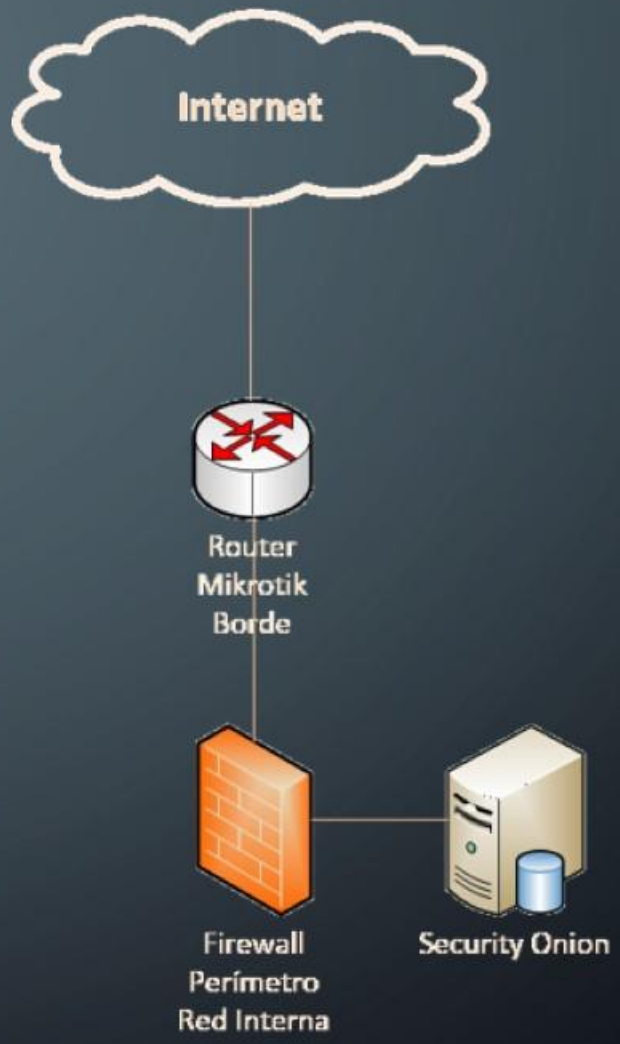
- Aclarando los escenarios



3D'S TELECOMMUNICATION

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



3D'S TELECOMMUNICATION

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

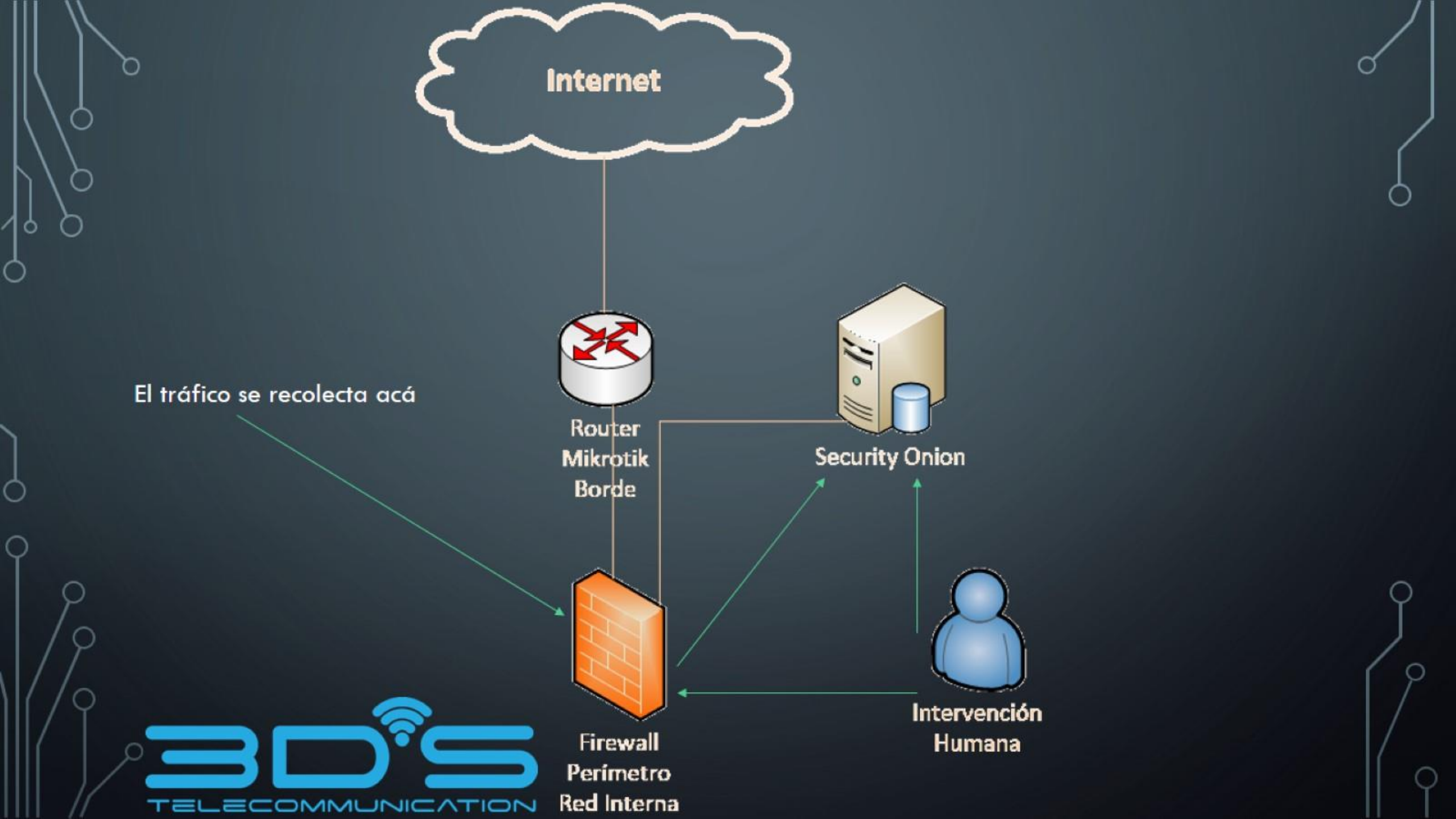
3D'S TELECOMMUNICATION

3D'S TELECOMMUNICATION

FUERA DE LÍNEA

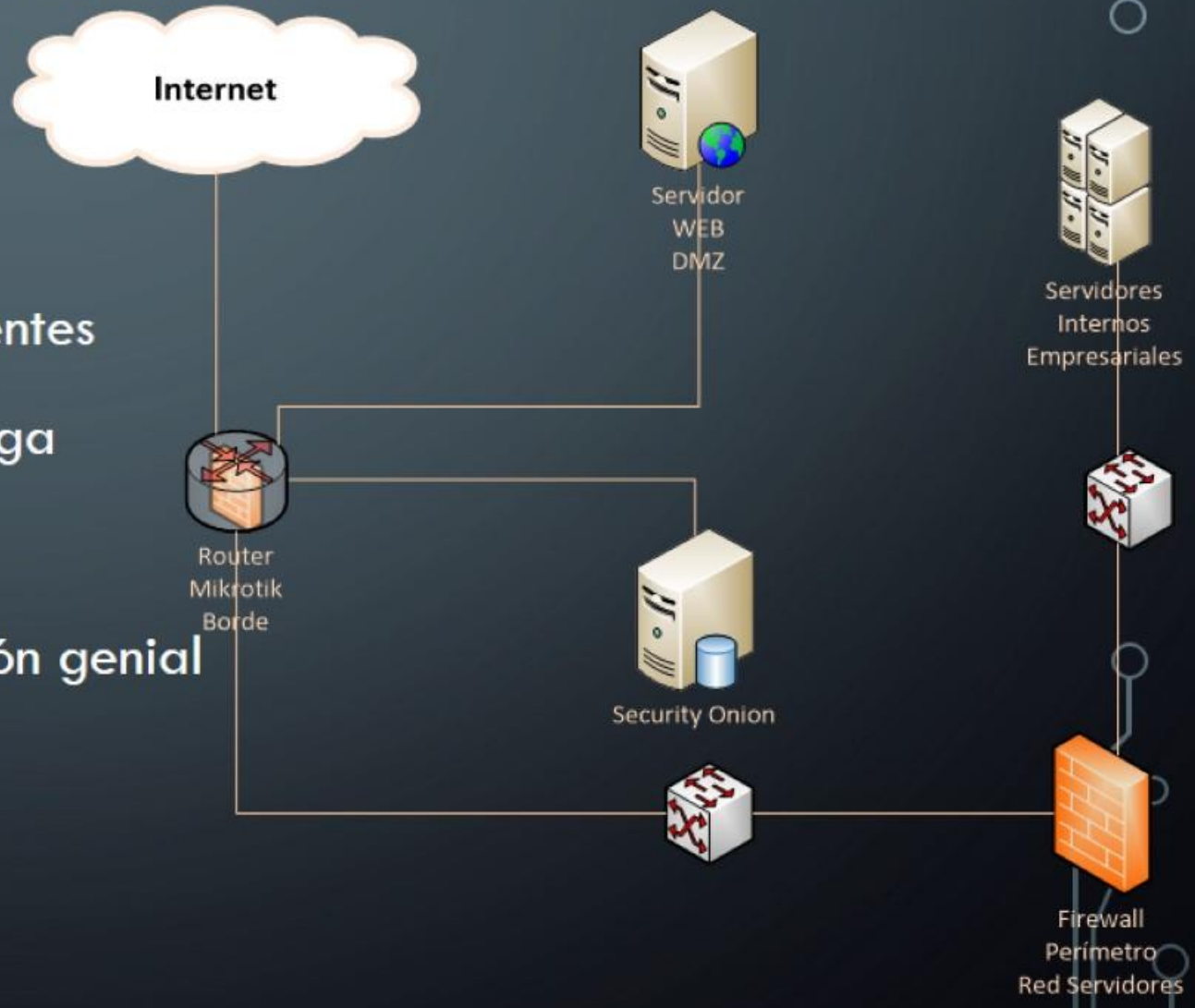
- El tráfico no pasa por el punto de análisis
- El tráfico cifrado no es inspeccionable
- Menor nivel de inspección
- Solo permite monitoreo, no acción (IDS)
- Una falla en el sistema IDS no afecta al tráfico

3D'S TELECOMMUNICATION


Internet
El tráfico se recolecta acá
Router
Mikrotik
Borde
Security Onion
Firewall
Perímetro
Red Interna
Intervención
Humana
3D'S
TELECOMMUNICATION

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



3D'S TELECOMMUNICATION

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

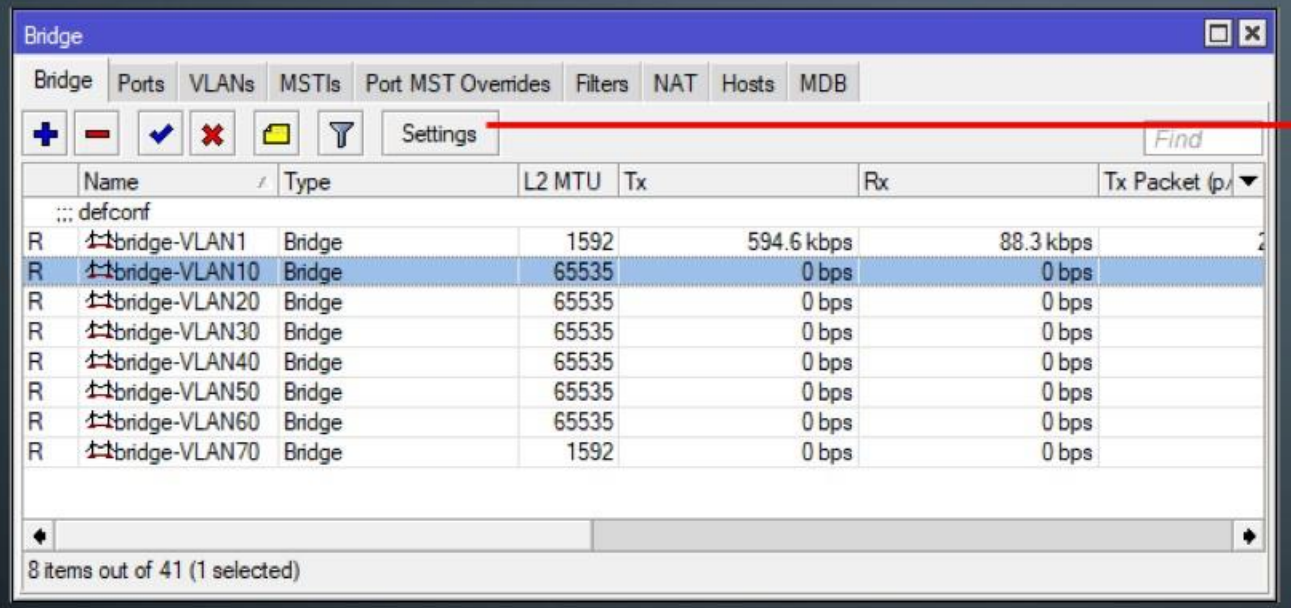
3D'S TELECOMMUNICATION

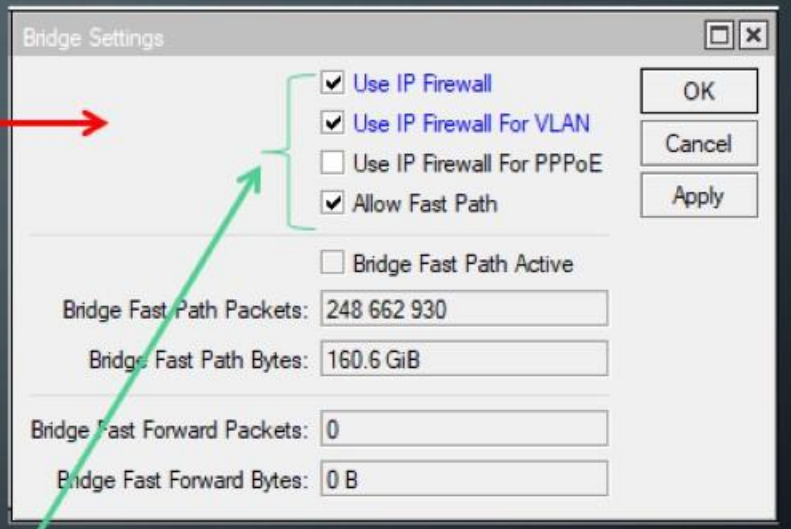
CONFIGURAR EL MIKROTIK

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

3D'S TELECOMMUNICATION

CONFIGURACIONES EN CAPA 2



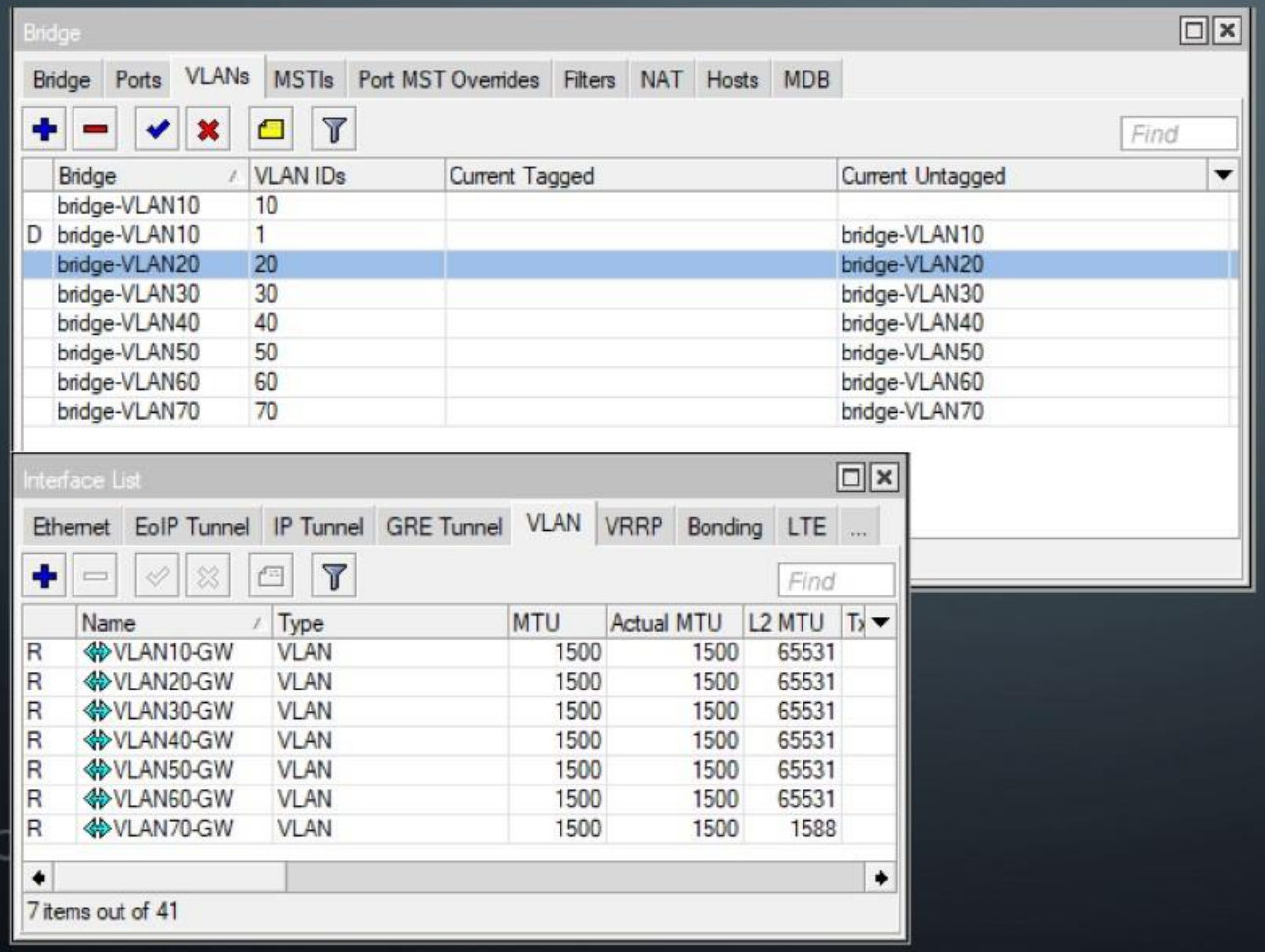


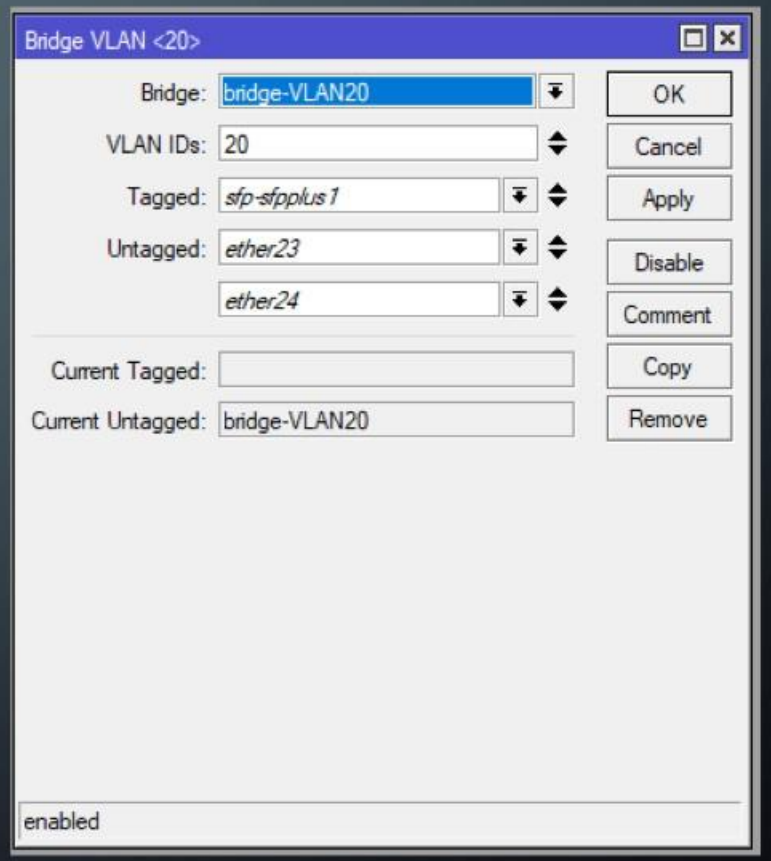
Activar estas opciones para manejar el tráfico

3D'S TELECOMMUNICATION

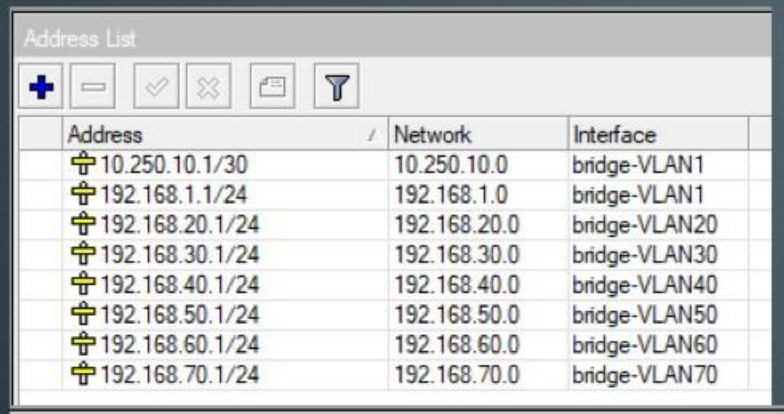
CONFIGURACIONES EN CAPA 2, CONT…

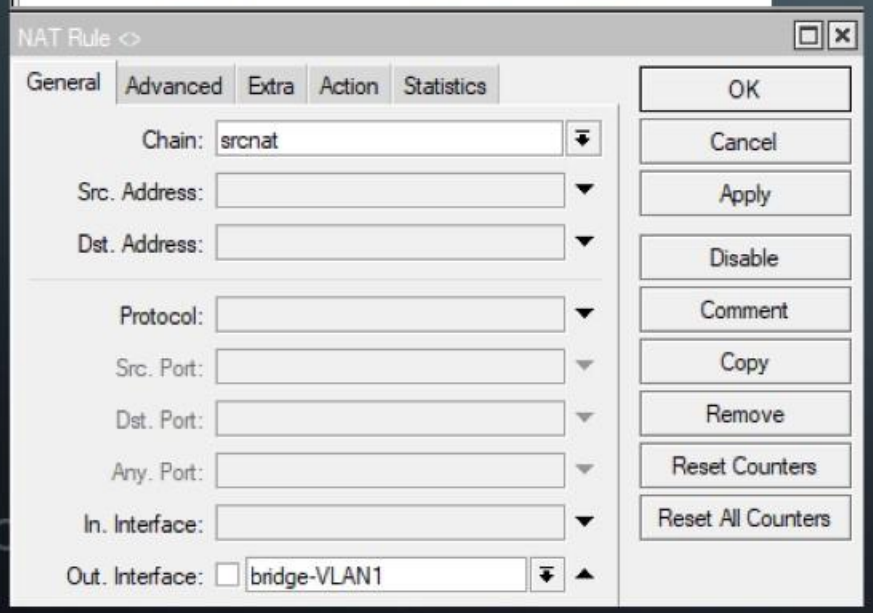
- Configuraciones de VLAN, Interfaces virtuales y puertos

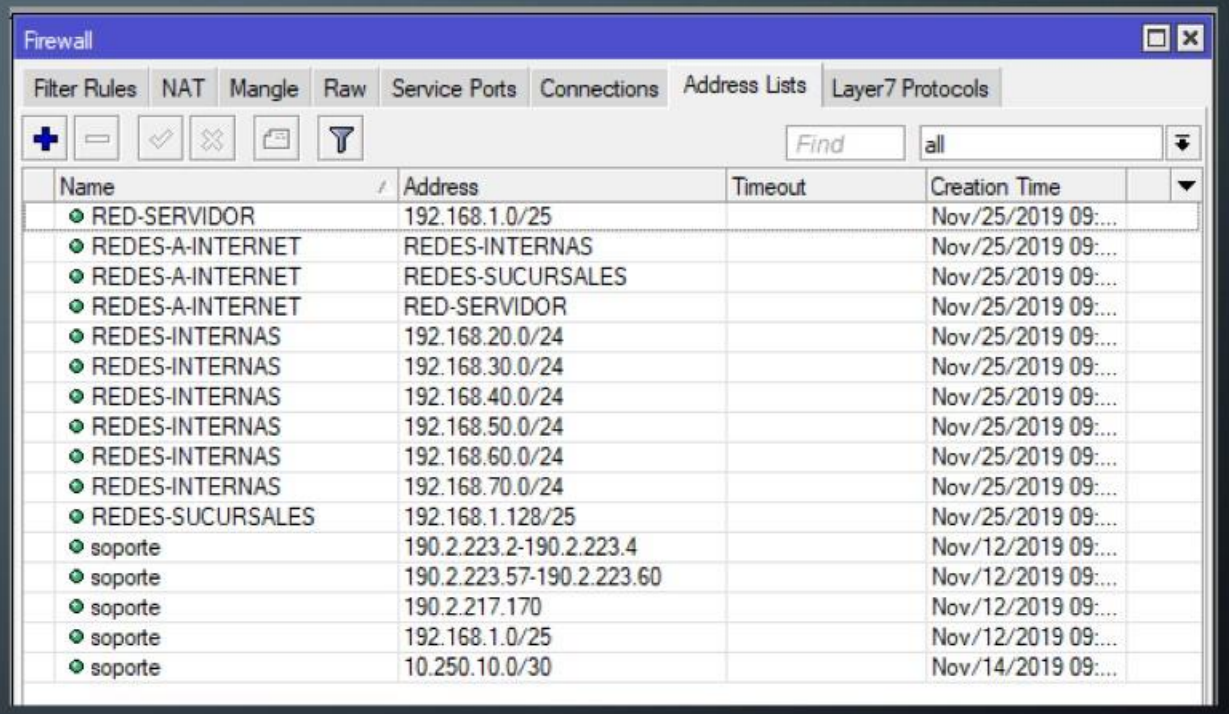




CONFIGURACIONES EN CAPA 3







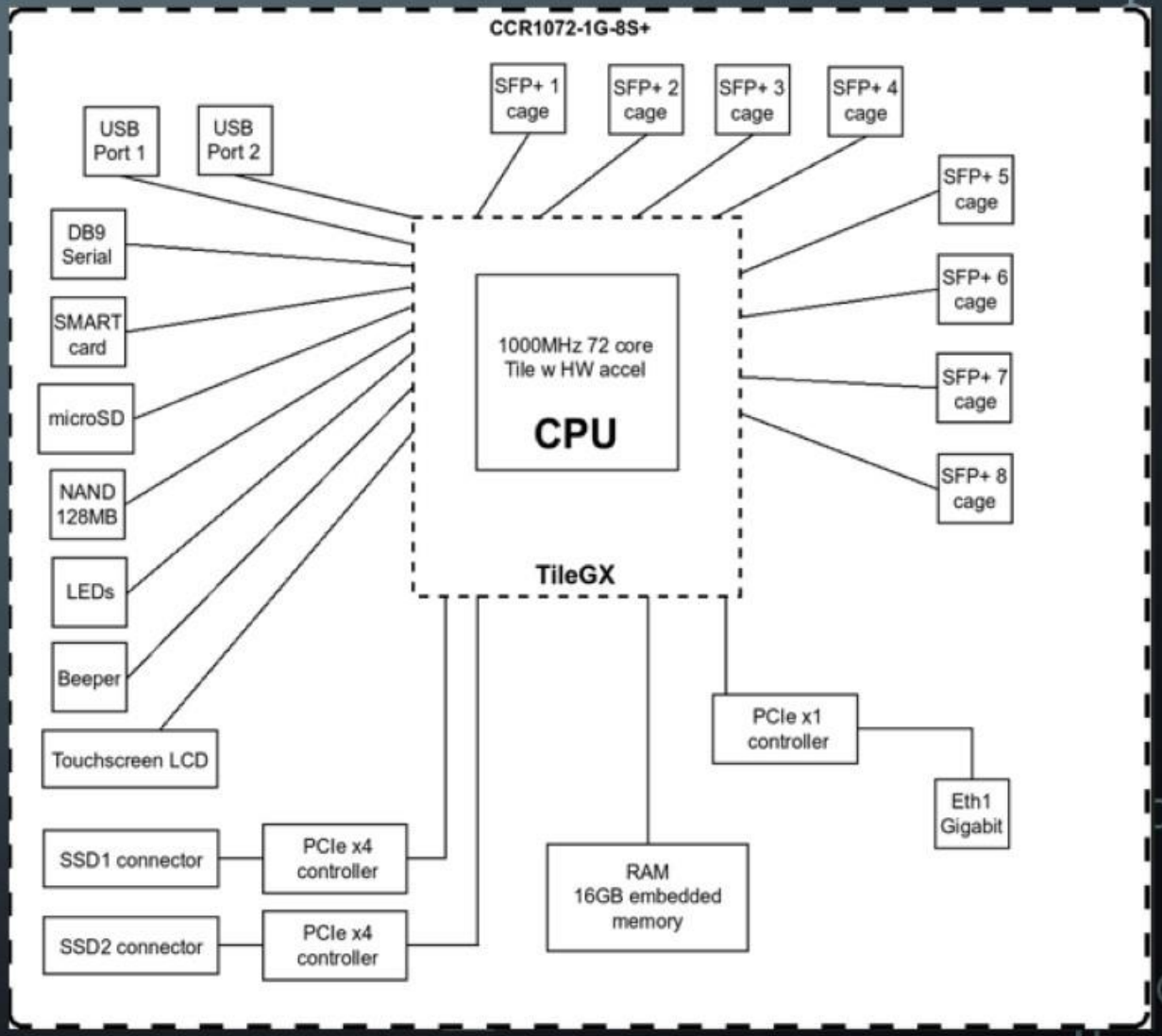
PORT MIRROR EN MIKROTIK

- 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

3D'S TELECOMMUNICATION

MODELO CCR1072-1G-8S+

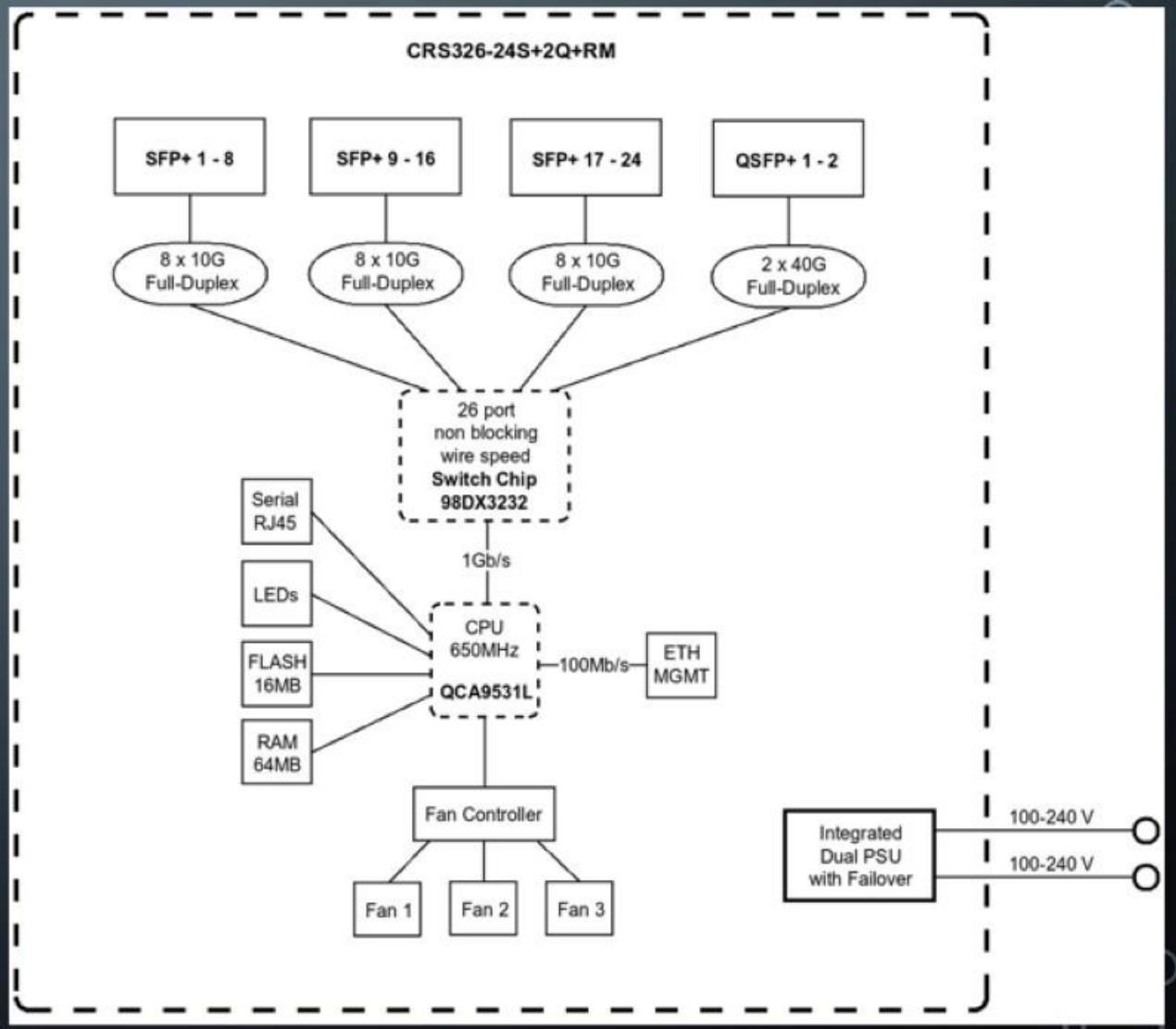
- Las funciones de switching (bridge) son asumidas por los CPUs.
- Todo es por software
- Rendimiento no optimizado



3D'S TELECOMMUNICATION

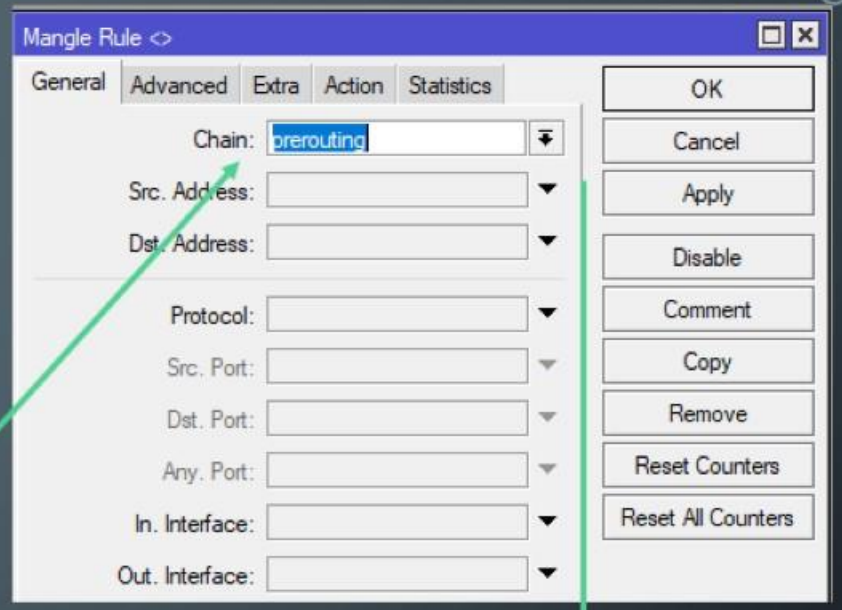
MODELO CRS326-24S+2Q+RM

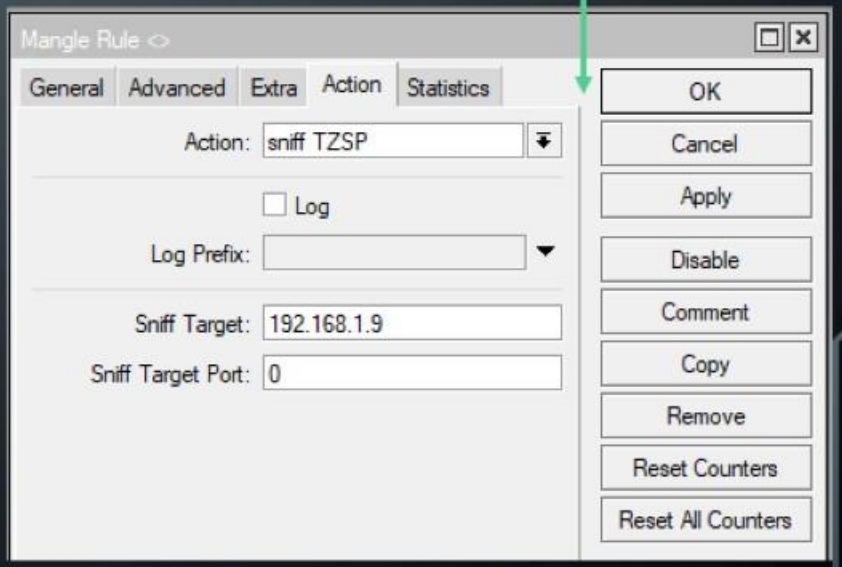
- Chipset especializado
- El CPU maneja el enrutamiento
- El switcheo por hardware
- Rendimiento optimizado

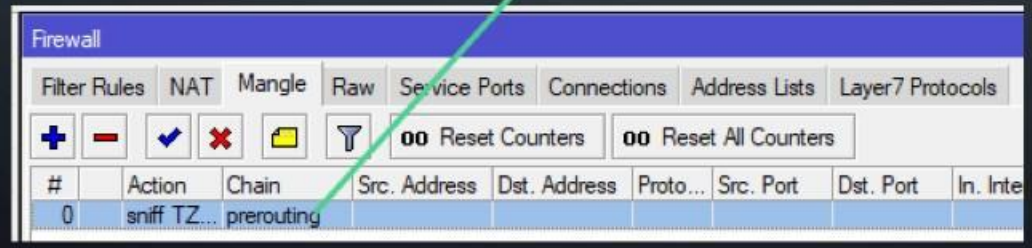


MANGLE

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

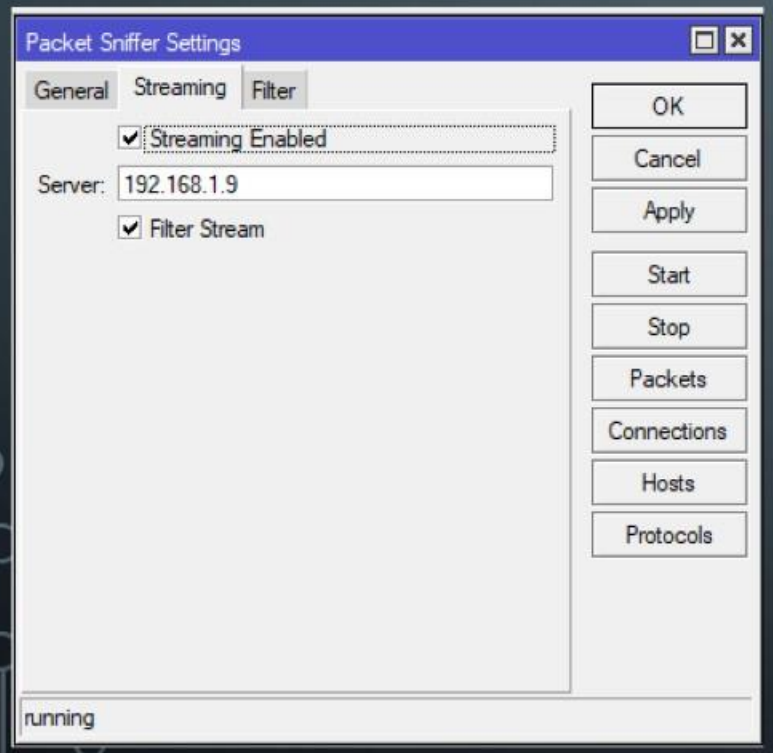


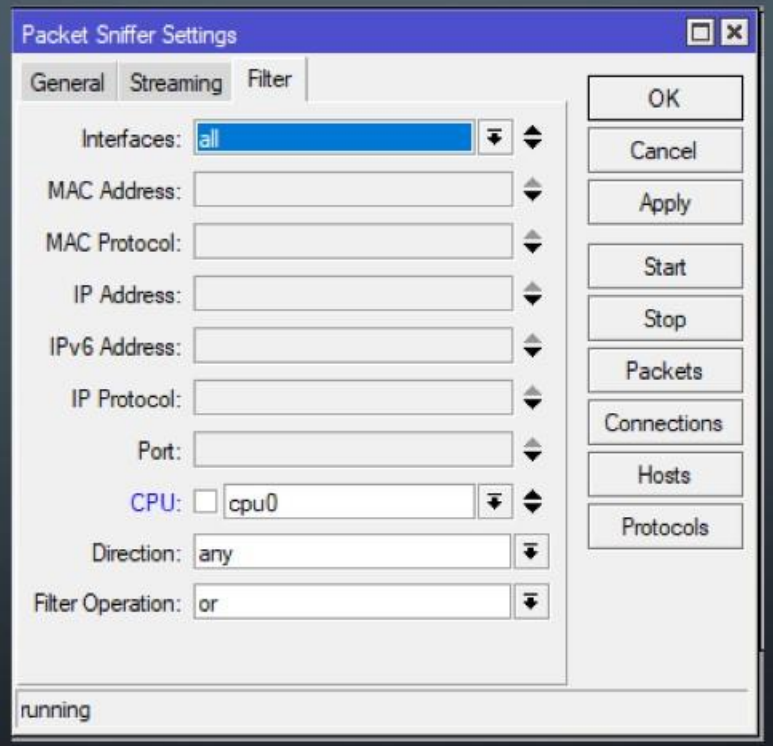


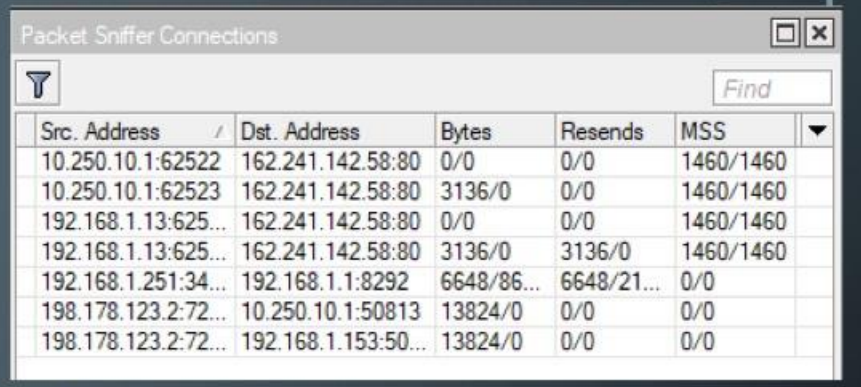


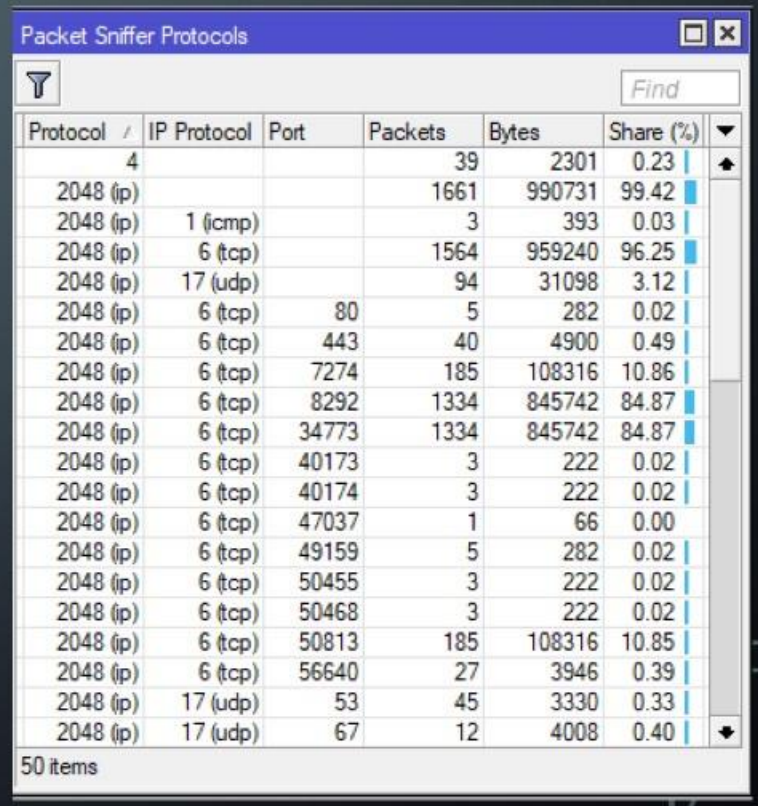
PACKET SNIFFER

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



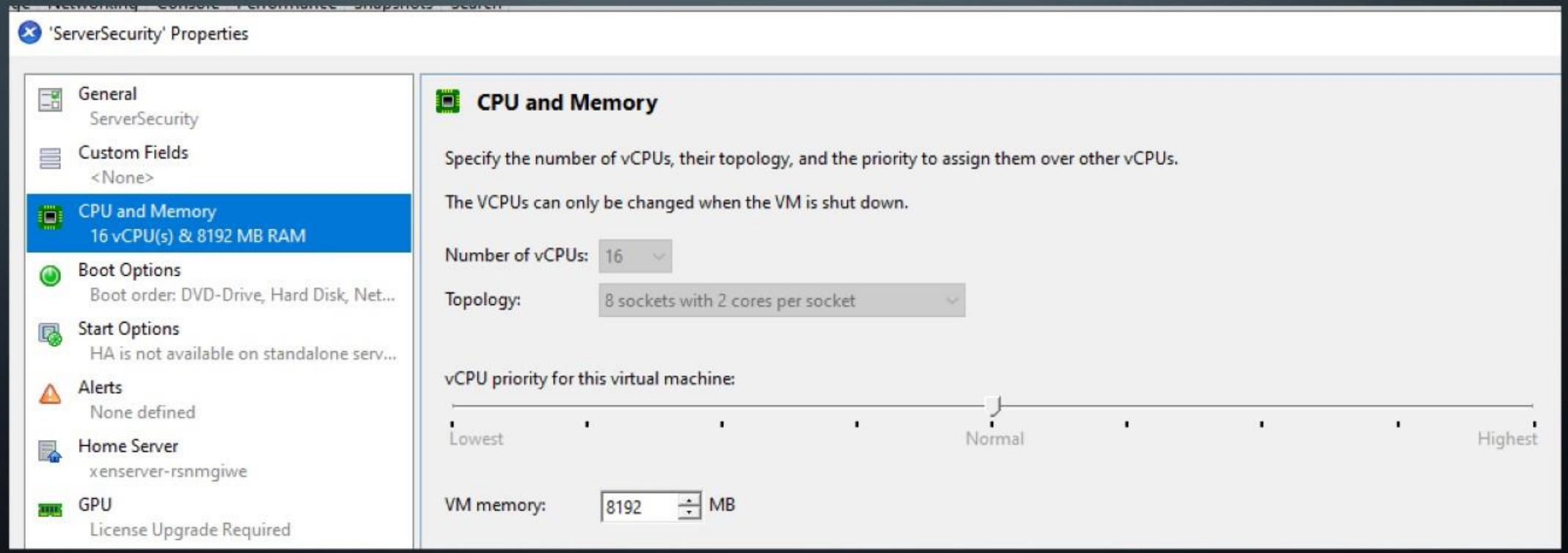






SECURITY ONION, EL ANÁLISIS

- Capacidad de procesamiento



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

3D'S TELECOMMUNICATION

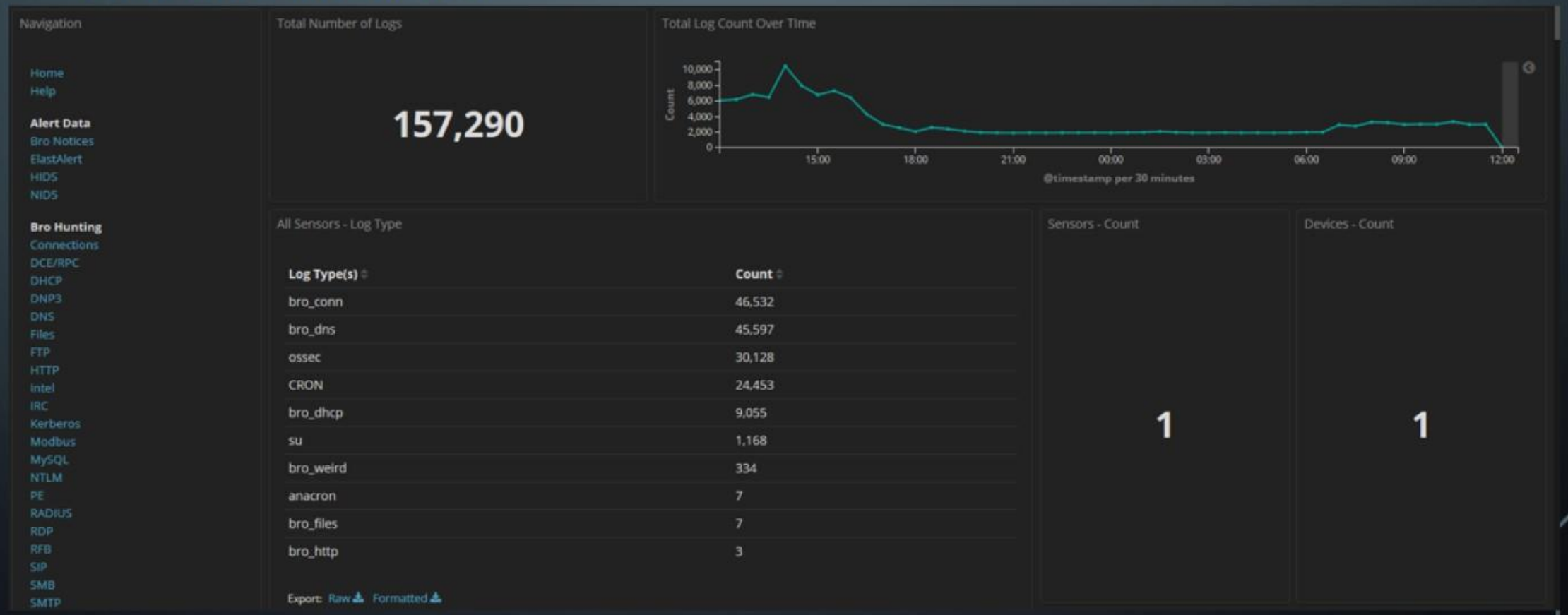
SURICATA/SNORT

INTRUSION DETECTION WITH SURICATA

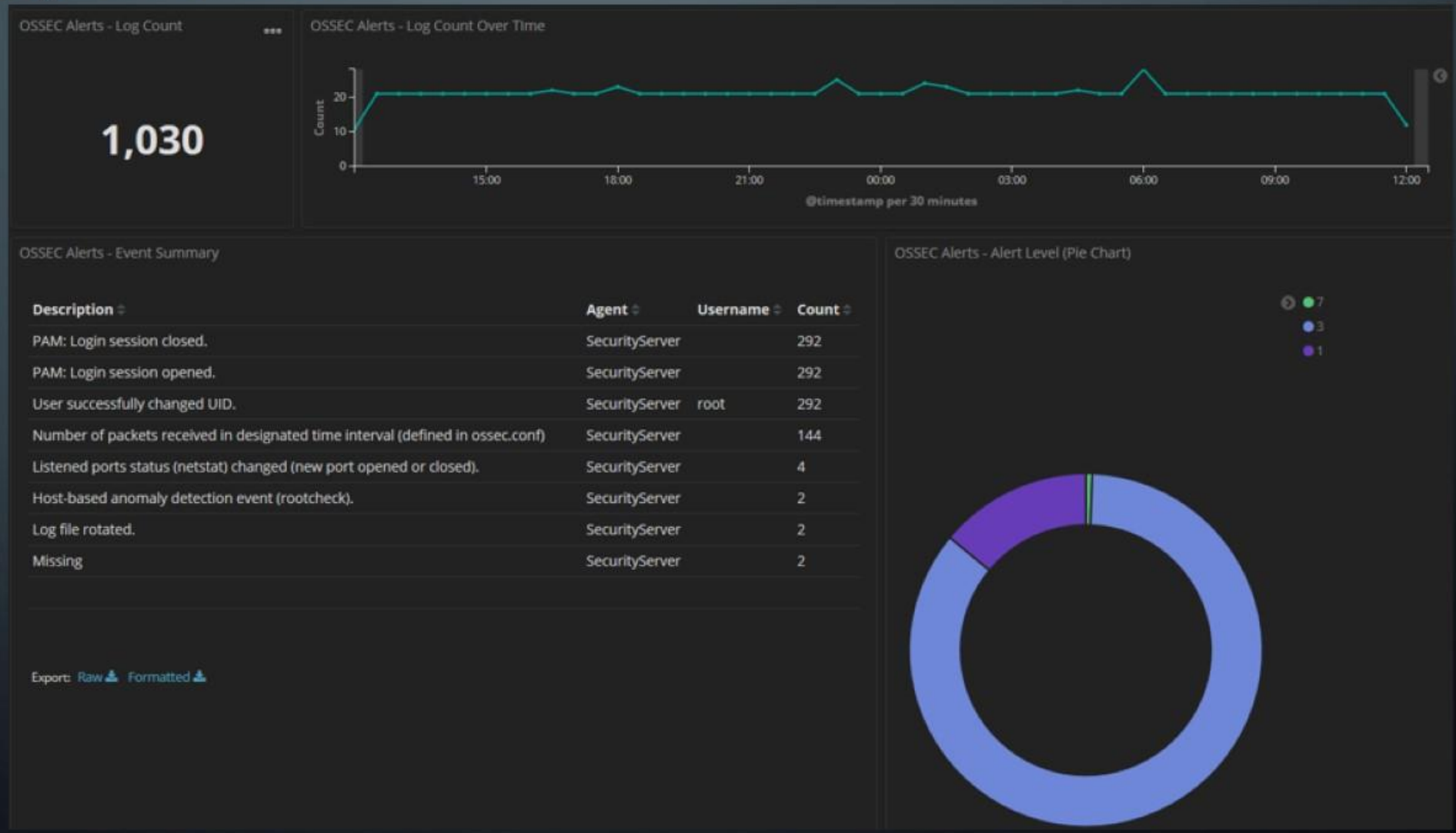
3D'S TELECOMMUNICATION

KIBANA

- Dashboard informativo



KIBANA, CONT…


OSSEC Alerts - Log Count
1,030
OSSEC Alerts - Log Count Over Time
Count
20
10
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
@timestamp per 30 minutes
OSSEC Alerts - Event Summary
Description
Agent
Username
Count
PAM: Login session closed. SecurityServer 292
PAM: Login session opened. SecurityServer 292
User successfully changed UID. SecurityServer root 292
Number of packets received in designated time interval (defined in ossec.conf) SecurityServer 144
Listened ports status (netstat) changed (new port opened or closed). SecurityServer 4
Host-based anomaly detection event (rootcheck). SecurityServer 2
Log file rotated. SecurityServer 2
Missing SecurityServer 2
Export: Raw Formatted
OSSEC Alerts - Alert Level (Pie Chart)
7
3
1

API MIKROTIK

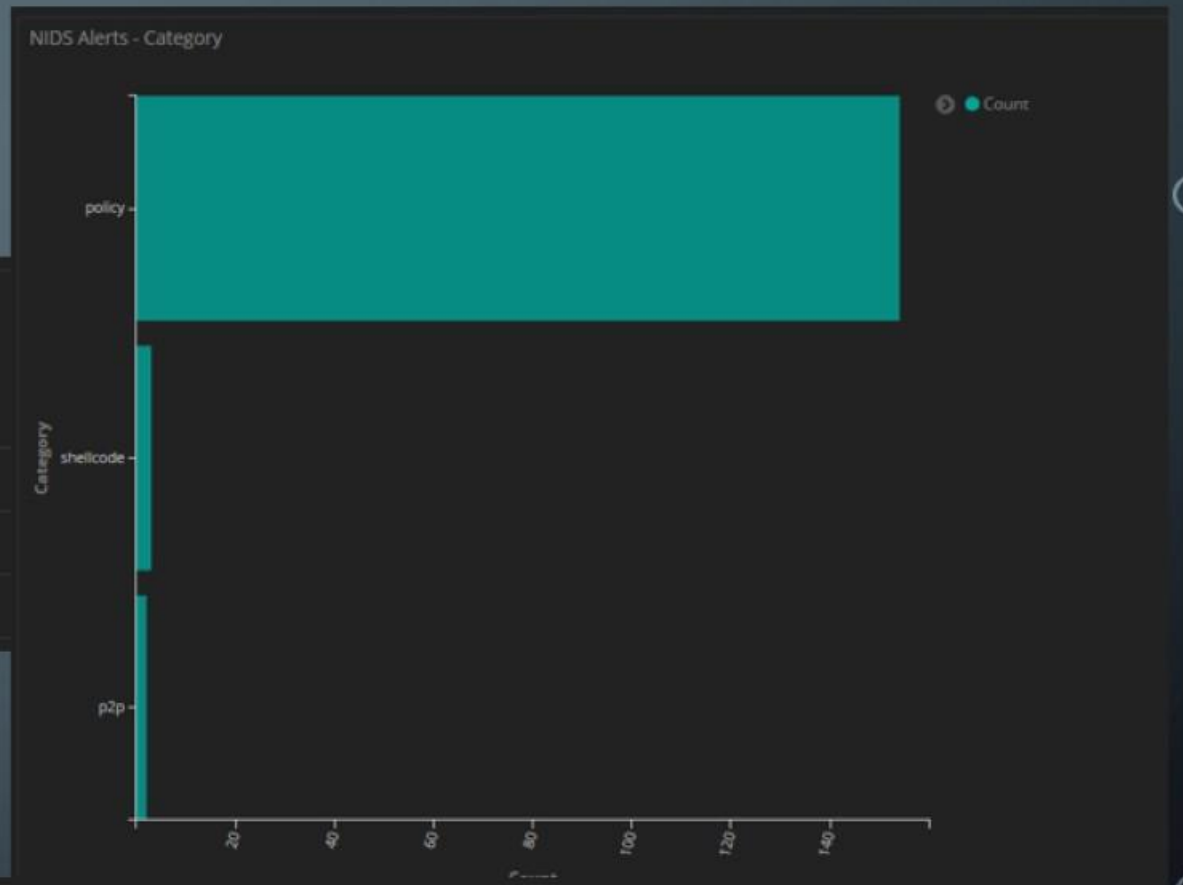
- Transformando nuestro IDS en un IPS
- Permite tomar el flujo de datos y enviarlos al servidor IPS/IDS Security Onion
- Security Onion tomas las decisiones acorde a su base de datos de firmas
- Dichas decisiones o triggers se envían al ROS mediante la API para generar los cambios en el firwall necesarios.

3D'S TELECOMMUNICATION

EJEMPLO

NIDS - Classification

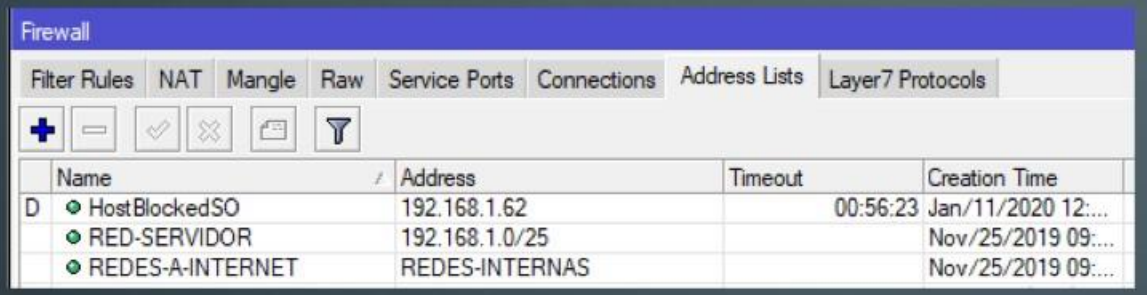
Classification	Count
Not Suspicious Traffic	154
Executable code was detected	3
Potential Corporate Privacy Violation	2

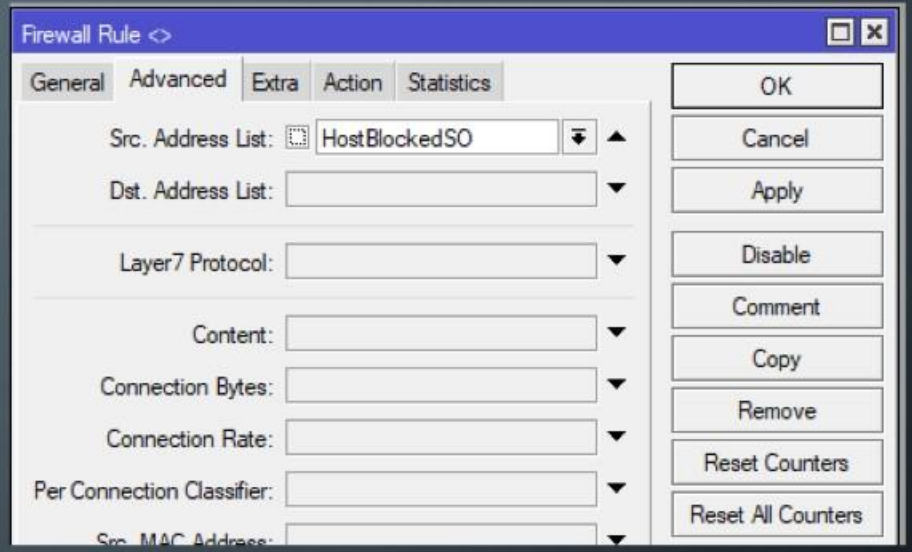


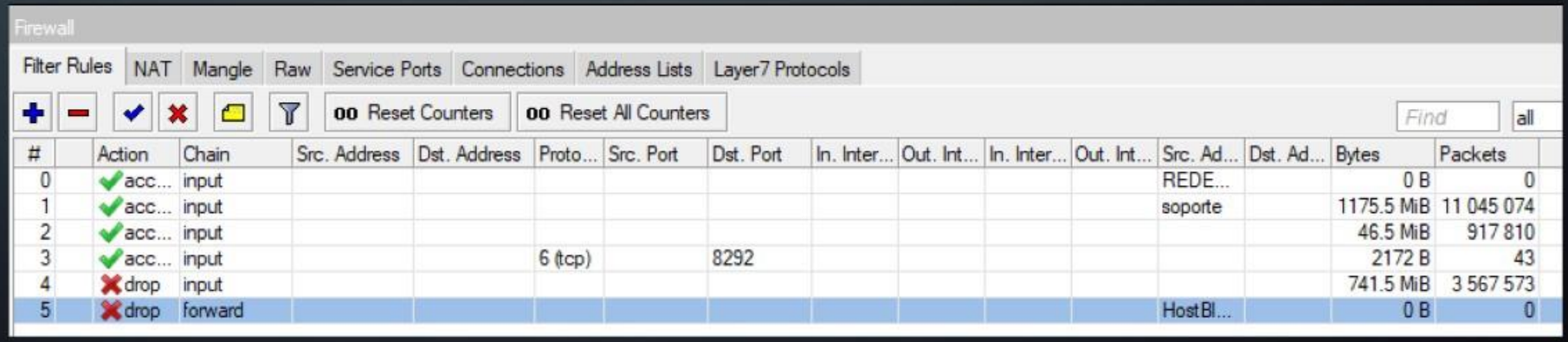
NIDS - Alert Summary

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…







Muchas GRACIAS