

# ¿QUÉ HAY EN TU RED?

Introducción a IDS/IPS...

# Agenda

1. ¿Qué es un IDS/IPS?
2. Estudio rápido de las soluciones IDS/IPS disponibles
3. Introducción a Security Onion
4. Práctica: Ejercicio

# ¿Qué es un IDS/IPS?

- Sistema de detección de intrusiones: sistema pasivo capaz de detectar, pero no mitigar, intrusiones en la red o en el host.
- Sistema de prevención de intrusiones: sistema activo capaz de detectar y de intervenir durante una intrusión en la red o en el host bloqueando o deteniendo la actividad maliciosa. Debe desplegarse en línea.

## Dos tipos principales de cada uno

Basado en la red: sistema conectado a una red o redes (NIDS y NIPS).

Basado en el host: software instalado en un servidor, máquina virtual o cliente que supervisa ese sistema específico en busca de actividad inesperada o maliciosa, como cambios en los archivos, tráfico de red, registros de errores, etc. (HIDS y HIPS).

# Métodos de detección

## IDS/IPS basados en el conocimiento y en firmas

Utiliza información de ataques previamente observados o publicado vulnerabilidades, por lo que estos sistemas sólo son capaces de detectar ataques o vulnerabilidades conocidos. También llamados "basados en reglas".

## IDS/IPS basados en el comportamiento y las anomalías

Funcionan estableciendo una línea de base y determinando después si el tráfico o las actividades no son normales\*. Estos tipos tienen la capacidad de detectar ataques hasta ahora desconocidos.

- Anomalía estadística: utiliza un sistema de puntuación para determinar el tráfico anómalo y generar alertas basadas en umbrales.
- Anomalía de tráfico: observa el tráfico dentro de una red y realiza determinaciones basadas en tendencias: volumen, uso de protocolos, etc.
- Anomalía de protocolo: busca desviaciones de la actividad normal del protocolo para detectar usos indebidos o abusos (por ejemplo, filtración de DNS).

Los sistemas IDS/IPS basados en anomalías requieren que se establezca una línea de base utilizando un periodo de entrenamiento para determinar qué es "normal". Ese periodo de entrenamiento puede ser de días, semanas o meses...

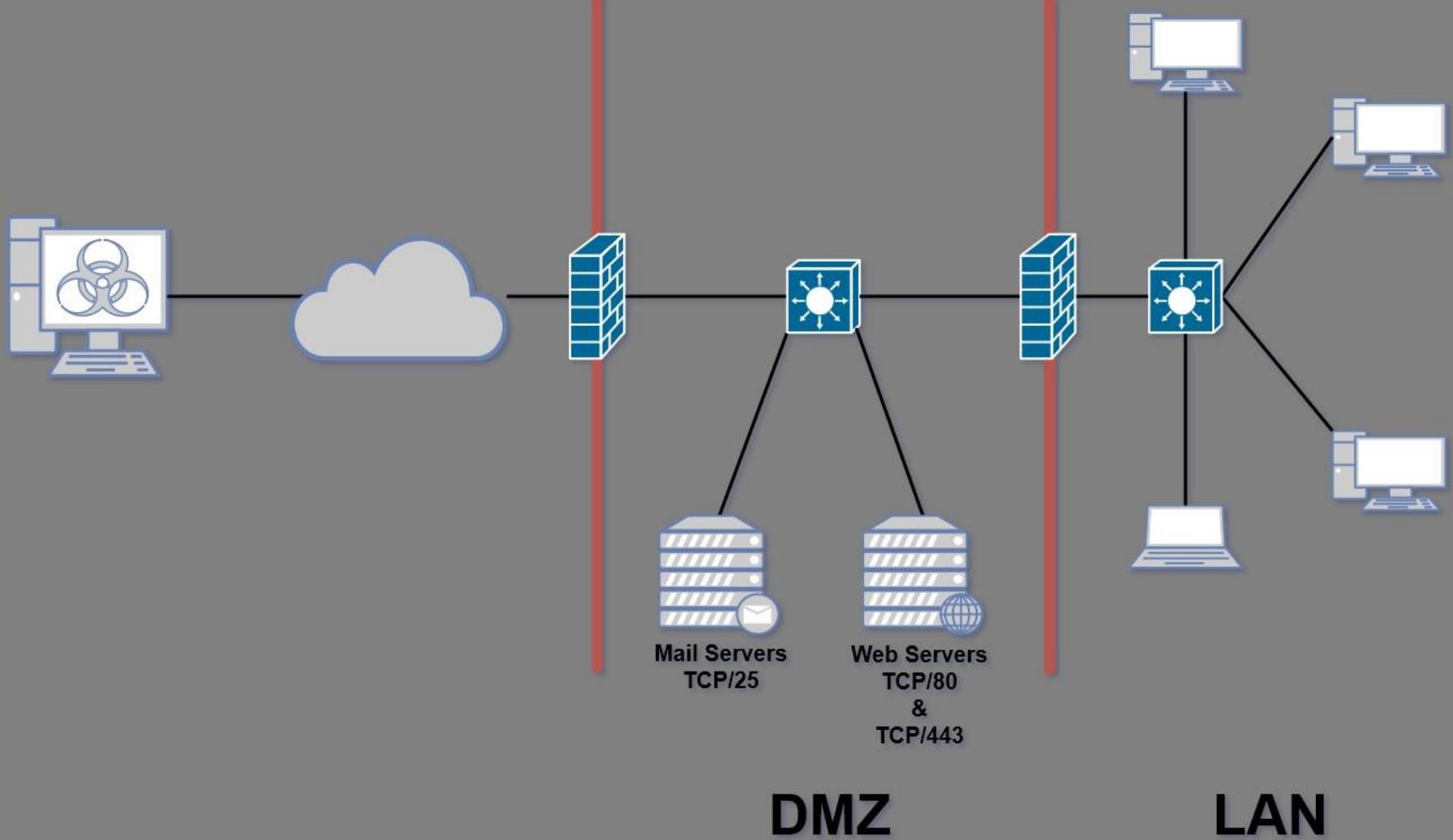
El tráfico malicioso puede clasificarse como...  
"Normal"

# Vale, pero, tengo un firewall...

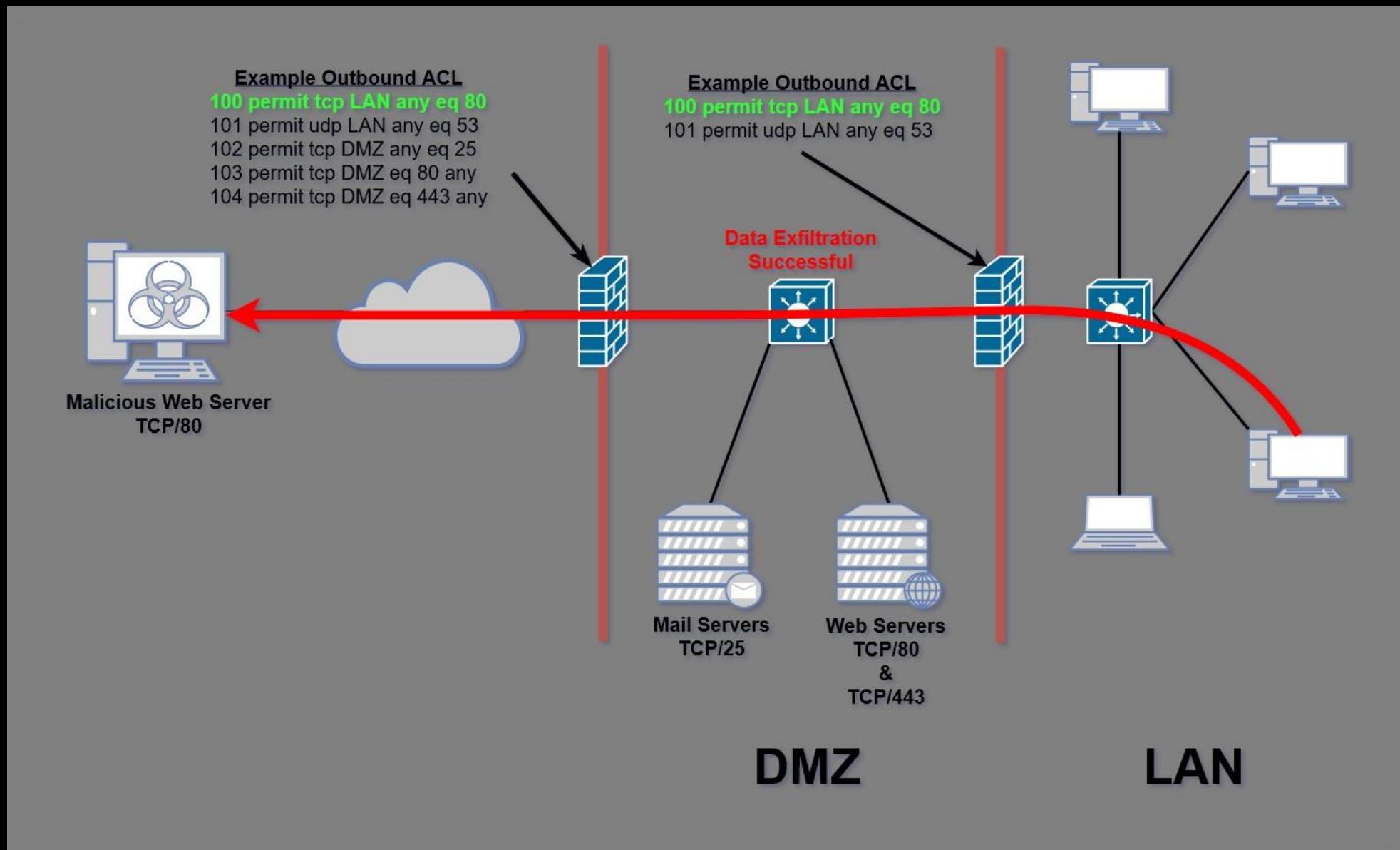
Los cortafuegos son excelentes para el filtrado de direcciones de origen/destino, puertos y protocolos, pero una protección más fina requiere algo más.

Veamos algunos ejemplos de cómo los cortafuegos pueden fallar en la protección por sí solos...

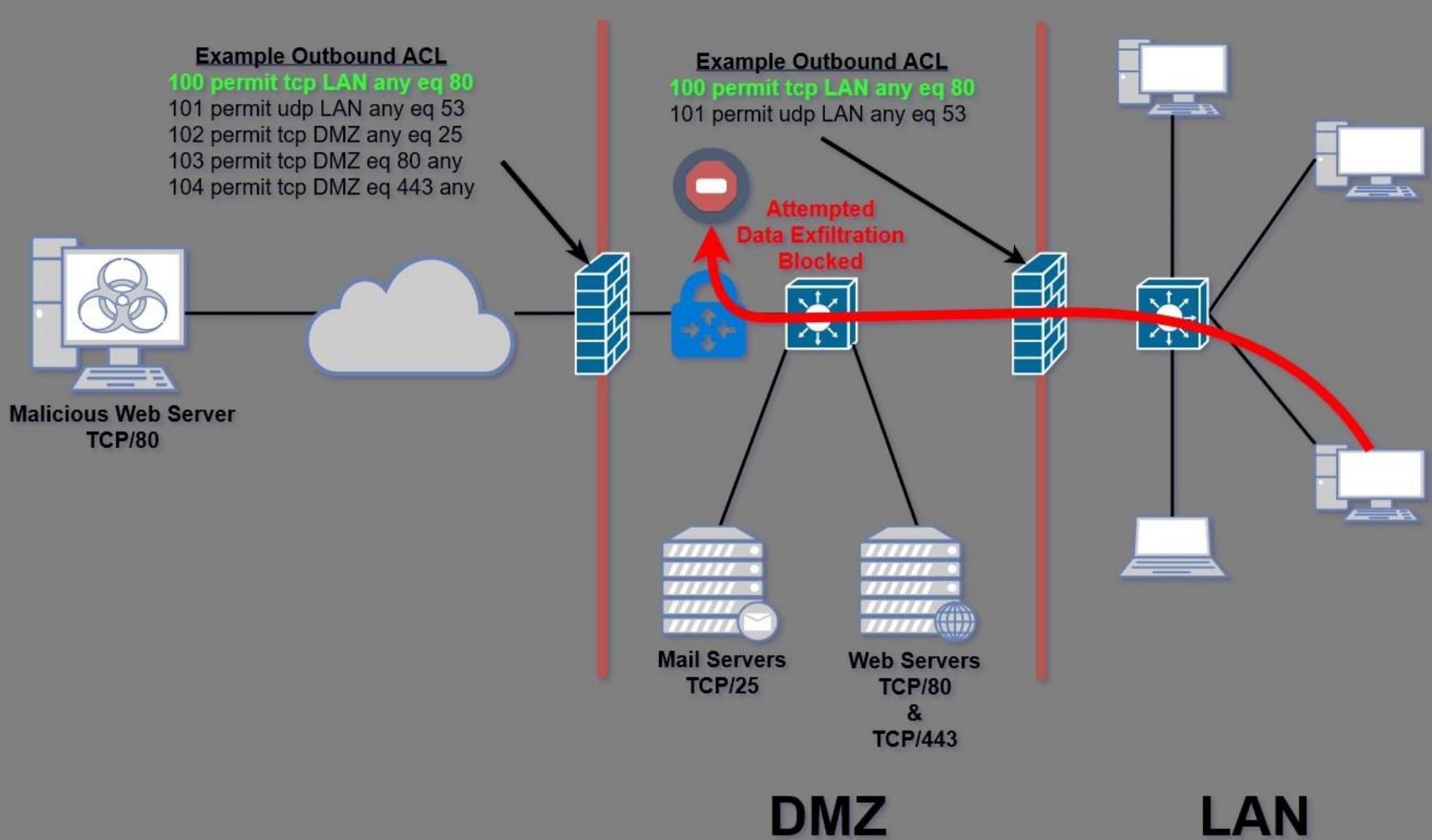
# Topología de red



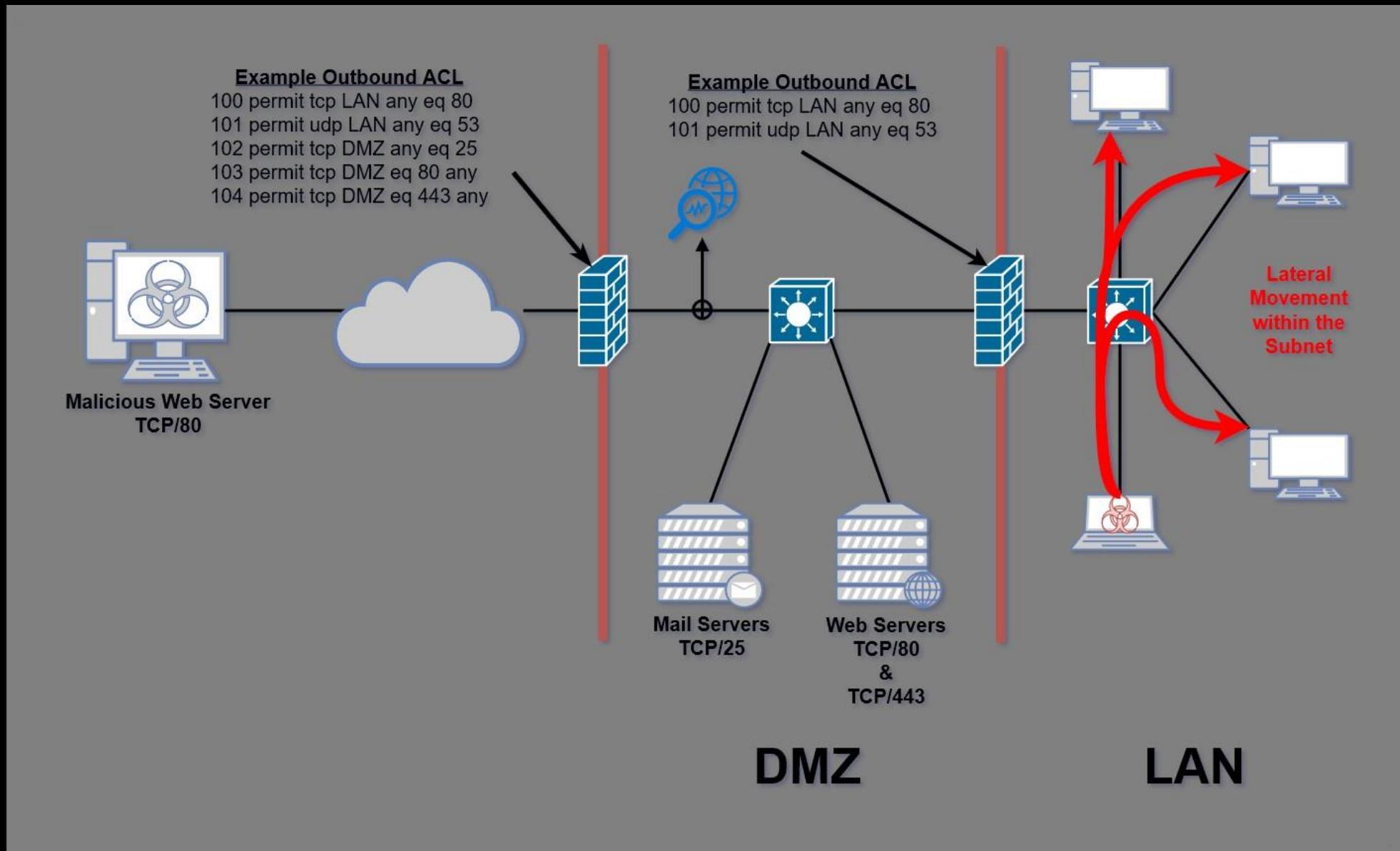
# Escenario 1: Solicitudes de salida



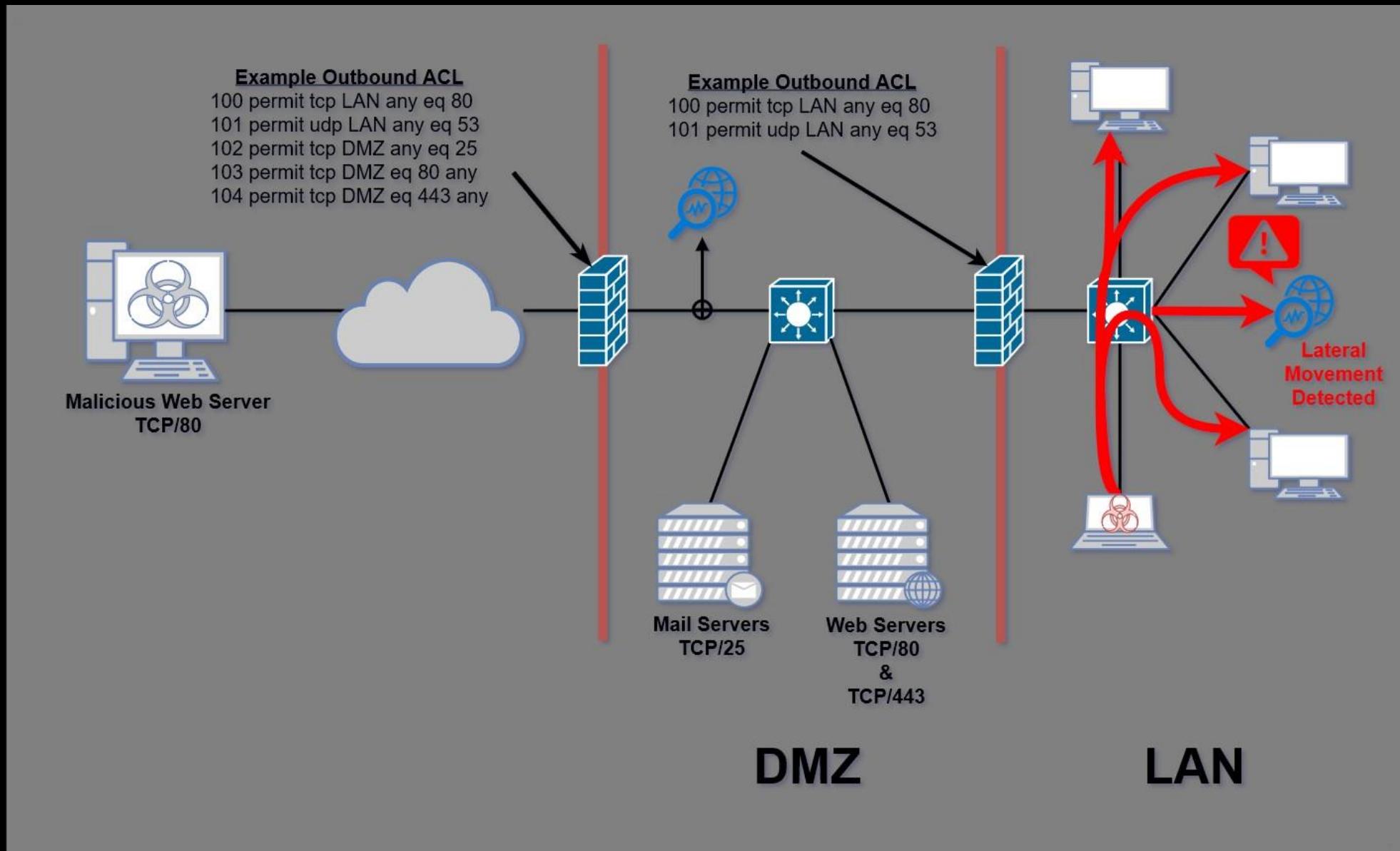
# Topología de despliegue: Exfiltración de datos (IPS)



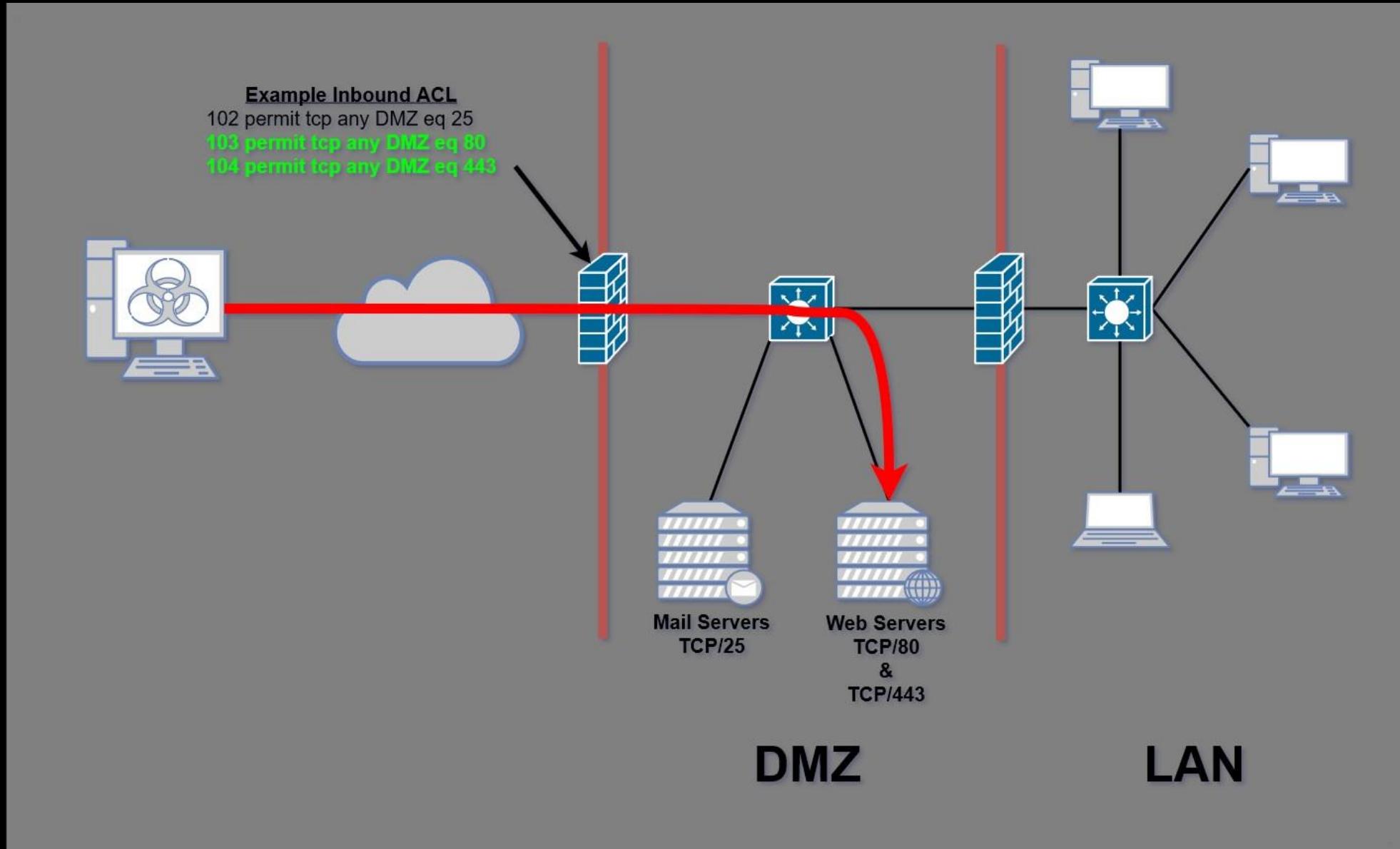
# Escenario 2: Tráfico de host a host ("Movimiento lateral")



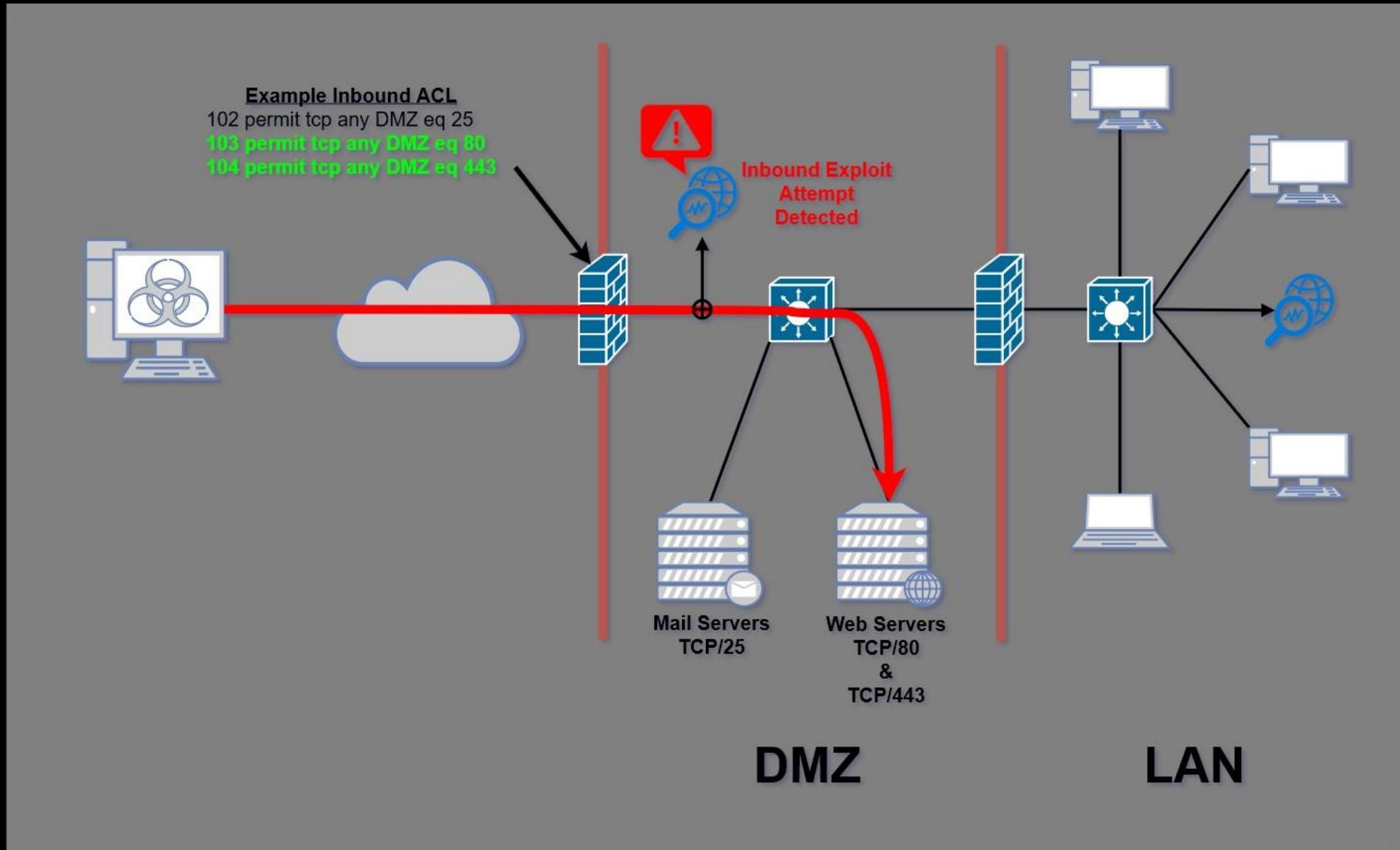
# Topología de despliegue: Movimiento lateral (con IDS)



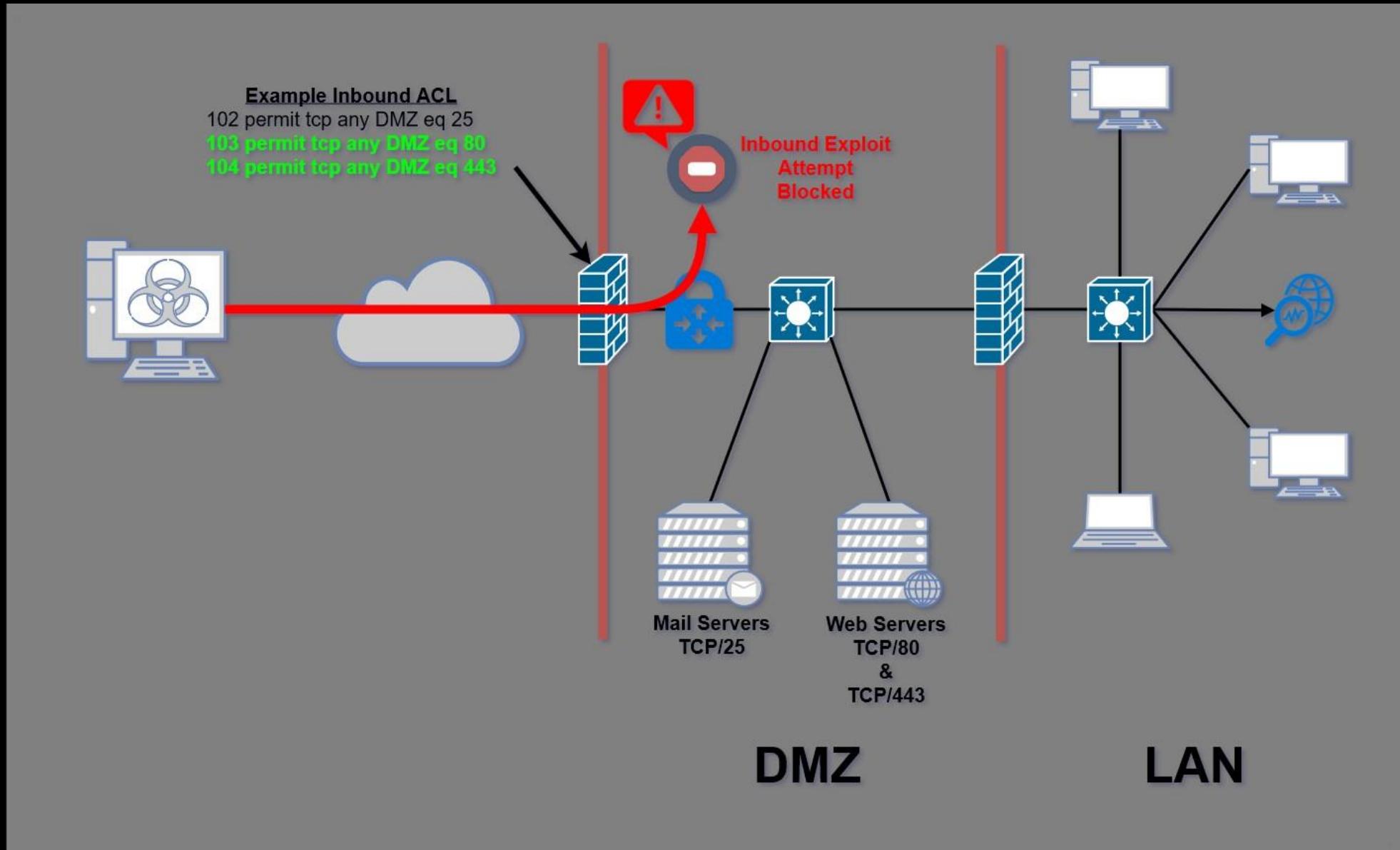
# Escenario 3: Peticiones entrantes al host DMZ



# Topología de despliegue: Ataque de entrada (IDS)



# Topología de despliegue: Ataque entrante (IPS)



¿Qué soluciones existen?

# Soluciones comerciales



TREND  
MICRO™

FORTINET®

IBM

McAfee™

CISCO

FireEye™

paloalto  
NETWORKS

ALERT LOGIC®

# "Alternativas "más baratas

## SOPHOS

### Línea SG (SG 135)

- Rendimiento FW de 6 Gbps
- 1 Gbps de rendimiento IDS/IPS
- < 2500 € (incluida la ayuda)



USG 3P	USG Pro	USG XG
Rendimiento >1 Gbps (sin procesar)	Rendimiento >1 Gbps (sin procesar)	Rendimiento >10 Gbps (sin procesar)
85 Mbps de rendimiento IDS/IPS	250 Mbps de rendimiento IDS/IPS	Rendimiento IDS/IPS de 1 Gbps
140 €	350 €	2500 €

# Interfaz Ubiquiti UniFi IDS/IPS

The screenshot displays the UniFi IDS/IPS dashboard with the following key components:

- World Map:** Shows threat activity across the globe, with a red arrow pointing to the United States.
- REAL-TIME THREATS:** A list of detected threats:
  - A Network Trojan was Detected
  - Potentially Bad Traffic
  - Potential Corporate Privacy Violation
  - Potentially Bad Traffic
  - Potential Corporate Privacy Violation
  - Potentially Bad Traffic
  - A Network Trojan was Detected
- Top Threats By Severity:** A donut chart showing the distribution of 78 total threats.

Severity	Count
High	68
Medium	10
Low	0
- Top Threats By Geo:** A table showing threats from the United States.

Source	Attempts	Severity
192.168.1.101	18	High
192.168.1.117	11	High
192.168.1.110	7	High
68.106.■■■■■	5	Medium
68.106.■■■■■	5	High
- Top Threats By Type:** A table showing threat types and their counts.

Type	Attempts	Severity
A Network Trojan was Detected	56	High
Potential Corporate Privacy Violation	11	High
Potentially Bad Traffic	10	Medium
Attempted User Privilege Gain	1	High
- Security Alerts:** A section showing a grid of alert cards, with a legend for severity: Low (blue), Medium (orange), and High (red).

Panel de visión general

# Interfaz Ubiquiti UniFi IDS/IPS

The screenshot displays the UniFi IDS/IPS dashboard. At the top, there's a navigation bar with icons for Unifi, Filter (0), Overview (selected), Traffic Log, and a date range of Last 24 Hours. On the left, a sidebar contains icons for Home, Devices, Threats, Logs, Reports, and Settings.

The main area features a world map with a red arrow pointing from North America towards the Atlantic Ocean. Below the map, a circular gauge shows "Total Threats" at 78, with segments for High (red), Medium (orange), and Low (green).

Below the gauge, three threat counts are listed:

Severity	Count
High	68
Medium	10
Low	0

On the right, there are two tables: "Top Threats By Geo" and "Top Threats By Type".

**Top Threats By Geo:**

Geo	Attempts	Severity	Source
United States	18	High	192.168.1.101
United States	11	High	192.168.1.117
United States	7	High	192.168.1.110
United States	5	Medium	68.106.■■■
United States	5	High	68.106.■■■

**Top Threats By Type:**

Type	Attempts	Severity
A Network Trojan was Detected	56	High
Potential Corporate Privacy Violation	11	High
Potentially Bad Traffic	10	Medium
Attempted User Privilege Gain	1	High

At the bottom, there's a section for "Security Alerts" which is currently empty. A legend indicates the severity levels: Low (green dot), Medium (orange dot), and High (red dot).

Panel de registro de tráfico

# Interfaz Ubiquiti UniFi IDS/IPS

THREAT DETAIL X

Threat Date/Time	Severity	Medium
11/20/2018 9:13 am	Time Since Attack	11h 23m 49s
	Source	218.255.170.7:55372
Traffic Detail	Country	Hong Kong
ET EXPLOIT AVTECH Unauthenticated Command Injection in DVR Devices	Destination	192.168.0.21:80
	Protocol	TCP

SUPPRESS SIGNATURE BLOCK BLACKLIST IP WHITELIST IP

Atacante intentando usar un exploit conocido contra el DVR de seguridad del cliente.

# Opciones independientes de FOSS

Basado en red



Bro / Zeek



Basado en host



Y otros...

# Bro / Zeek

<http://www.bro.org/>



Vern Paxson comenzó a desarrollarlo en 1994 en la Universidad de Berkeley.

Más que una solución IDS estándar: realiza un análisis en profundidad del tráfico de red para identificar amenazas, posibles vulnerabilidades o paquetes de software y sistemas obsoletos.

Por ejemplo, Bro puede analizar cadenas de agente de usuario para detectar navegadores o versiones de Java obsoletos. También puede monitorizar conexiones SSL/TLS para identificar certificados caducados o autofirmados.

En 2018, el equipo directivo de Bro decidió cambiar el nombre del proyecto a "Zeek" [http://blog.bro.org/2018/10/renaming-bro-project\\_11.html](http://blog.bro.org/2018/10/renaming-bro-project_11.html)

# Snort



<http://www.snort.org/>

Martin Roesch, fundador de SourceFire, comenzó a desarrollarlo en 1998.

En 2013, Cisco compró SourceFire, utilizando Snort como base de la función FirePower IDS; Snort independiente sigue siendo de código abierto.

El motor de Snort está escrito en C. Hasta la versión 3.0, que ahora está en Beta, Snort era monohilo, lo que requería múltiples procesos para escalar.

Cisco, Proofpoint y Crowdstrike producen reglas "en tiempo real" compatibles, todas ellas mediante suscripción. La suscripción a las reglas VRT de Cisco proporciona las mismas reglas utilizadas en los dispositivos Firepower. Una suscripción personal a VRT cuesta 29 dólares al año. También existen las reglas Snort para usuarios registrados de forma gratuita, pero con un retraso de 30 días respecto a las reglas VRT de pago. Las reglas Snort Community también son gratuitas, pero carecen de reglas VRT.

# Suricata

- <http://www.suricata-ids.org/>
- El desarrollo de Suricata está liderado por OISF, la Fundación Abierta para la Seguridad de la Información. La primera versión de producción se publicó en 2010.
- Suricata fue diseñado para abordar algunas de las deficiencias percibidas en Snort. Por ejemplo, Suricata es multihilo por defecto.
- El conjunto de reglas preferido para Suricata son las reglas de Amenazas Emergentes (Abierto y de pago), pero es capaz de usar muchas reglas de Snort. Algunas de Las reglas de objetos compartidos ("compiladas") no son compatibles con Suricata.
- Una desventaja de Suricata es que la documentación está menos desarrollada que la de Snort y tiene una comunidad de usuarios más pequeña.



# Tripwire



<https://github.com/Tripwire/tripwire-open-source>

La versión de código abierto de Tripwire se basa en código aportado por Tripwire, Inc. en 2000. La versión comercial de el software Tripwire sigue existiendo.

Tripwire es un sistema de monitorización de la integridad de los archivos que detecta cambios en una lista de archivos o ficheros del sistema operativo configurada por el usuario. Cuando se modifica un archivo, Tripwire genera una alerta.

# OSSEC

<http://www.ossec.net/>

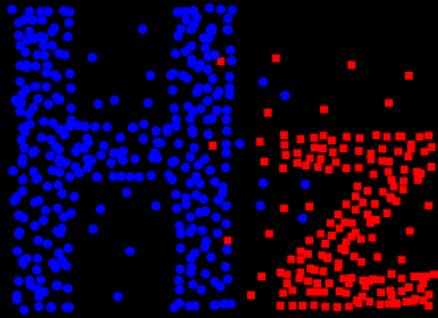
El desarrollo comenzó en 2005  
de la mano de Daniel Cid.



Los derechos del proyecto fueron finalmente adquiridos por Trend Micro en 2009, pero el desarrollo del proyecto continúa y sigue siendo de código abierto.

OSSEC es un HIDS multiplataforma que funciona en \*BSD, Linux y Windows, y tiene capacidad para supervisar varios sistemas desde un único host centralizado. OSSEC ofrece análisis de registros, supervisión de integridad de archivos, aplicación de políticas, detección de rootkits, alertas y respuesta activa.

# Hogzilla



<http://ids-hogzilla.org>

Primera edición -  
2016\*

The screenshot shows a log entry in the GrayLog interface. The log details an event received by Hogzilla on IP 5b960318 at 2016-10-13 19:42:46.723. The event is stored in index graylog\_25. The log message is as follows:

```
dns_reverse
full_message
This IP was detected by Hogzilla performing an abnormal activity. In what follows, you can see more information.
Abnormal behaviour: Atypical alien TCP/UDP port used (5555)
IP: 5b960318
Bytes Up: 15.0MB
Bytes Down: 143.1MB
Total packets: 170
Flows matching the atypical ports
    24:55550 <--> 139:5555 [!] (TCP, L-to-R: 3.1MB, R-to-L: 0 B, 27 pkts, duration: 4494s, sampling: 1/2048)
    124:55319 <--> 16:5555 [!] (TCP, L-to-R: 128.0KB, R-to-L: 0 B, 1 pkts, duration: 0s, sampling: 1/2048)
ip
level
4
message
HZ: Atypical alien TCP port used - 24.
priority
WARNING
reference
http://ids-hogzilla.org/signature-db/826001004
sensor_hostname
Hogzilla
signature
HZ: Atypical alien TCP port used
source
timestamp
2016-10-13T22:42:46.723Z
```

"Hogzilla es un sistema de detección de intrusiones (IDS) de código abierto compatible con Snort, SFlows, GrayLog, Apache Spark, HBase y libnDPI, que proporciona **detección de anomalías en la red.**"

\*<https://www.linkedin.com/pulse/hogzilla-anomaly-based-ids-first-usable-release-alves-resende/>

Hacerlo uno mismo es una opción, pero...

Configurar, afinar y ajustar cada uno de ellos puede ser complejo.

Aunque construirlos desde cero es una buena forma de aprender, existen opciones para desplegar un IDS/IPS de código abierto mucho más rápidamente.

# Opciones "llave en mano"



Bro, Snort o Suricata,  
OSSEC, ElasticSearch,  
Logstash, Kibana y otros.

## BriarIDS

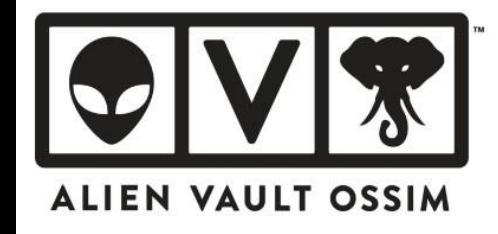
Bro y Suricata en  
la plataforma RPi  
(y algunos routers)

## Sweet Security

Bro, ElasticSearch, Logstash,  
Kibana y Critical Stack  
en la plataforma RPi

## pfSense

IDS/IPS mediante paquetes adicionales



Principalmente un sistema SIEM  
con IDS, OpenVAS, Nagios,  
Funciones de supervisión de  
Netflow

## SELKS

Suricata, ElasticSearch,  
Logstash, Kibana,  
Scirius, Evebox

Y posiblemente otros proyectos más  
pequeños...



[www.securityonion.net](http://www.securityonion.net)

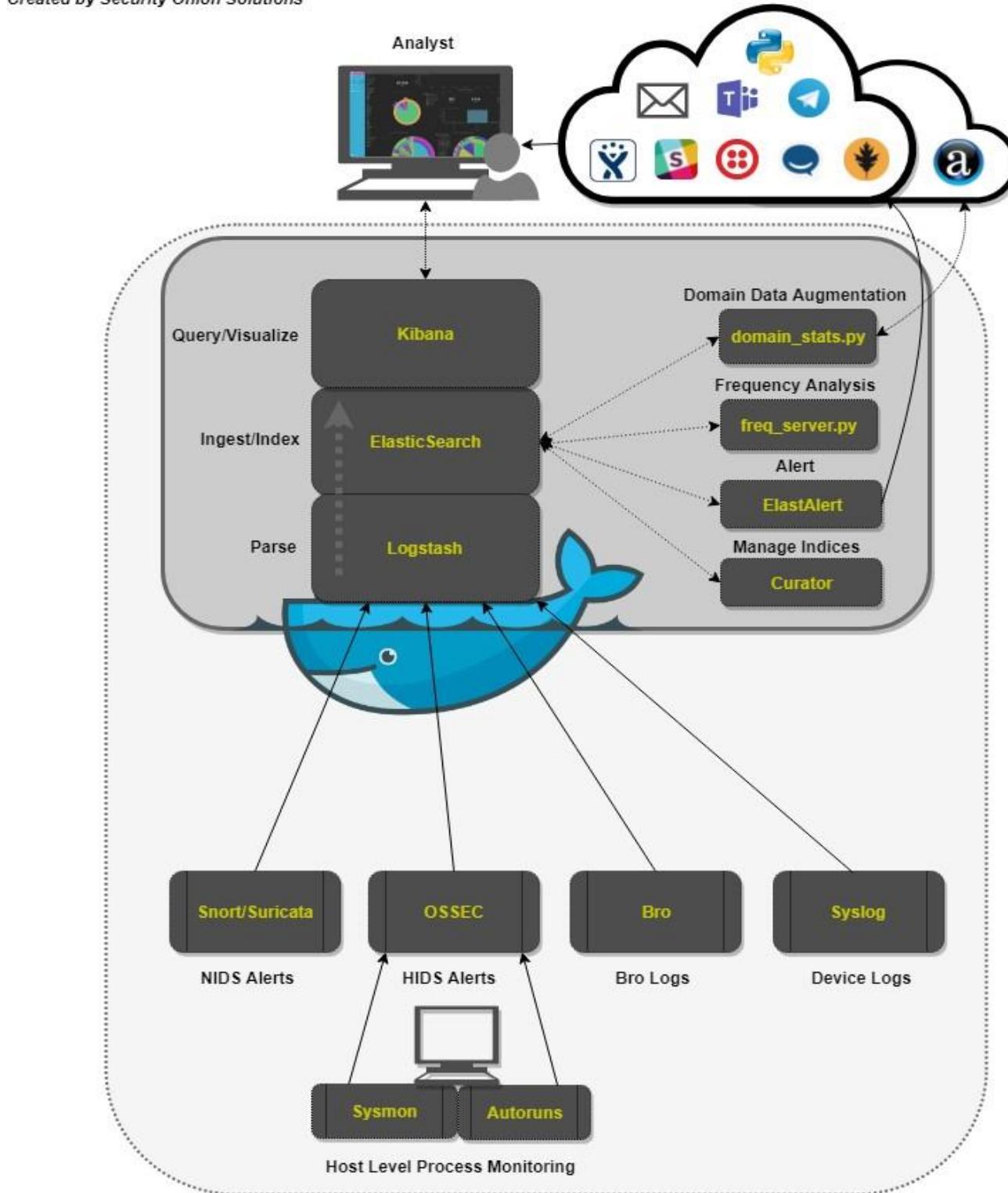


Doug Burks creó Security Onion en 2008, con la primera versión en 2009. En 2012, la distro fue reconstruida desde cero para mejorar su rendimiento y escalabilidad. Puede instalarse a partir de una ISO precompilada creada en Ubuntu o instalarse en una distro Ubuntu o similar a Ubuntu utilizando paquetes

Security Onion incluye las siguientes funciones:

- Bro/Zeek
- Snort y Suricata
- OSSEC (con agentes disponibles para varios sistemas operativos)
- ¡La pila ELK (Elasticsearch, Logstash y Kibana)
- capME!
- Consolas squil y squert
- Wireshark y NetworkMiner

**Security Onion - High-Level Architecture Diagram**  
Created by Security Onion Solutions



# Tipos de implantación

## Todo en uno

Todos los servicios de la pila Security Onion se alojan en una única máquina o VM. Aunque no están pensados para configuraciones de "producción", los despliegues "todo en uno" son aceptables para demostraciones y entornos pequeños, como tu casa.

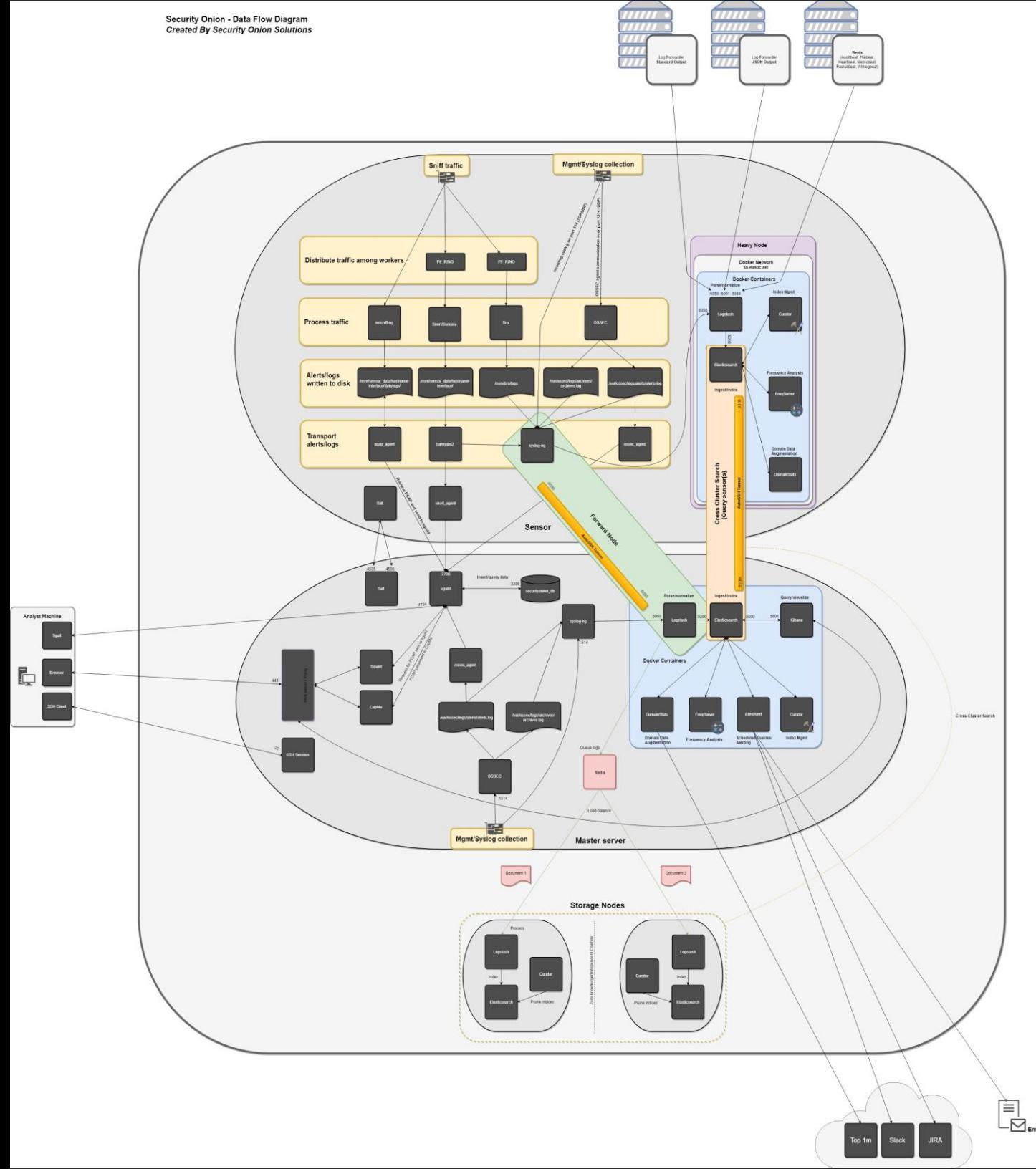
## Distribuido

Tres tipos de nodos para distribuir la carga de procesamiento a fin de escalar a grandes entornos y altos volúmenes de tráfico de red.

*Nodo de reenvío (sensor)*: Captura paquetes de la red y registros de los hosts.

*Nodo maestro*: Ejecuta las interfaces de analista (squid y squert) y los procesos de búsqueda/conservación de los registros recibidos.

*Nodos de almacenamiento*: Almacena e indexa registros y datos reenviados desde los sensores para ampliar las capacidades de almacenamiento y búsqueda del Nodo Maestro.



# Requisitos del sistema

## Requisitos mínimos del sistema

CPU de 64 bits

CPU mínima: 4 núcleos

RAM mínima: 8 GB

Un mínimo de dos interfaces de red

(Una para administración/actualizaciones y otra para captura de paquetes)

El espacio de almacenamiento depende de la velocidad a la que se capturan los paquetes o se ingieren los registros. Por ejemplo, una red con una media de 1Mbps de tráfico generará ~324GB de PCAPs al mes; 10Mbps son ~3,25TB.

Se necesitan más núcleos de CPU y RAM a medida que aumenta el rendimiento.

## Guía detallada de dimensionamiento

<https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware>

# Requisitos de la red

Para enviar paquetes a Security Onion y otras soluciones IDS, debe disponer de (1) un switch capaz de SPAN\* o duplicación de puertos o (2) una toma de red.

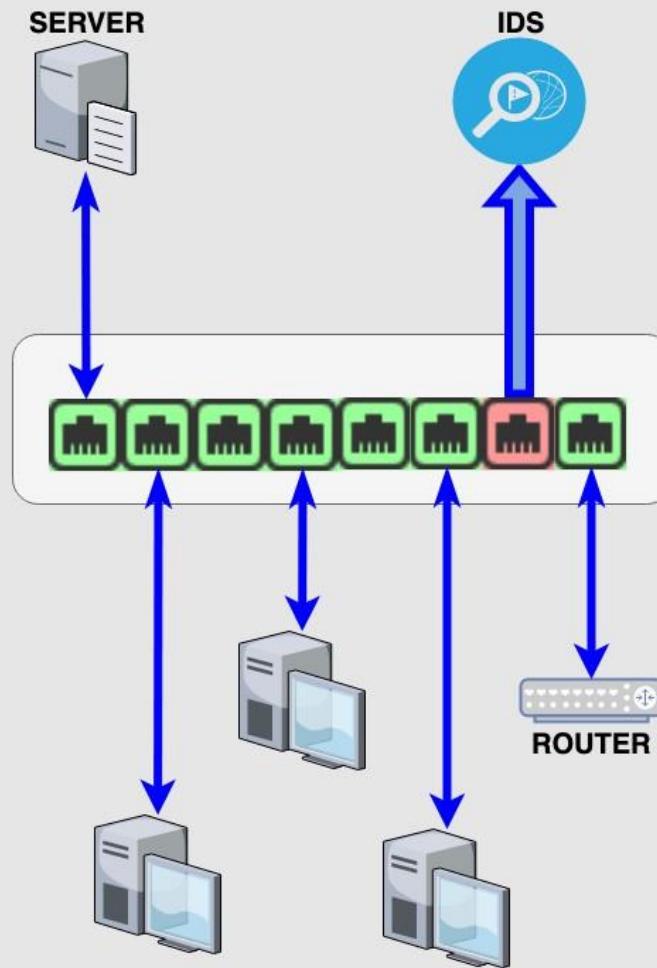
El despliegue de Security Onion como IPS requiere que el sistema se despliegue en línea (más allá del alcance de esta presentación introductoria).

## SPAN / Duplicación de puertos

Un conmutador toma todas las tramas Ethernet transmitidas/recibidas en un puerto o puertos y reenvía una copia fuera de un puerto o puertos Ethernet configurados.

Esta función sólo está presente en los switches gestionados.

\*SPAN - Analizador de puertos commutados



# Commutadores con capacidad de duplicación

Sólo algunas de las opciones...

D-Link DGS-1210-10

~90 €

Linksys LGS308

~80 €

Netgear GS108E

~70 €

(elección popular)

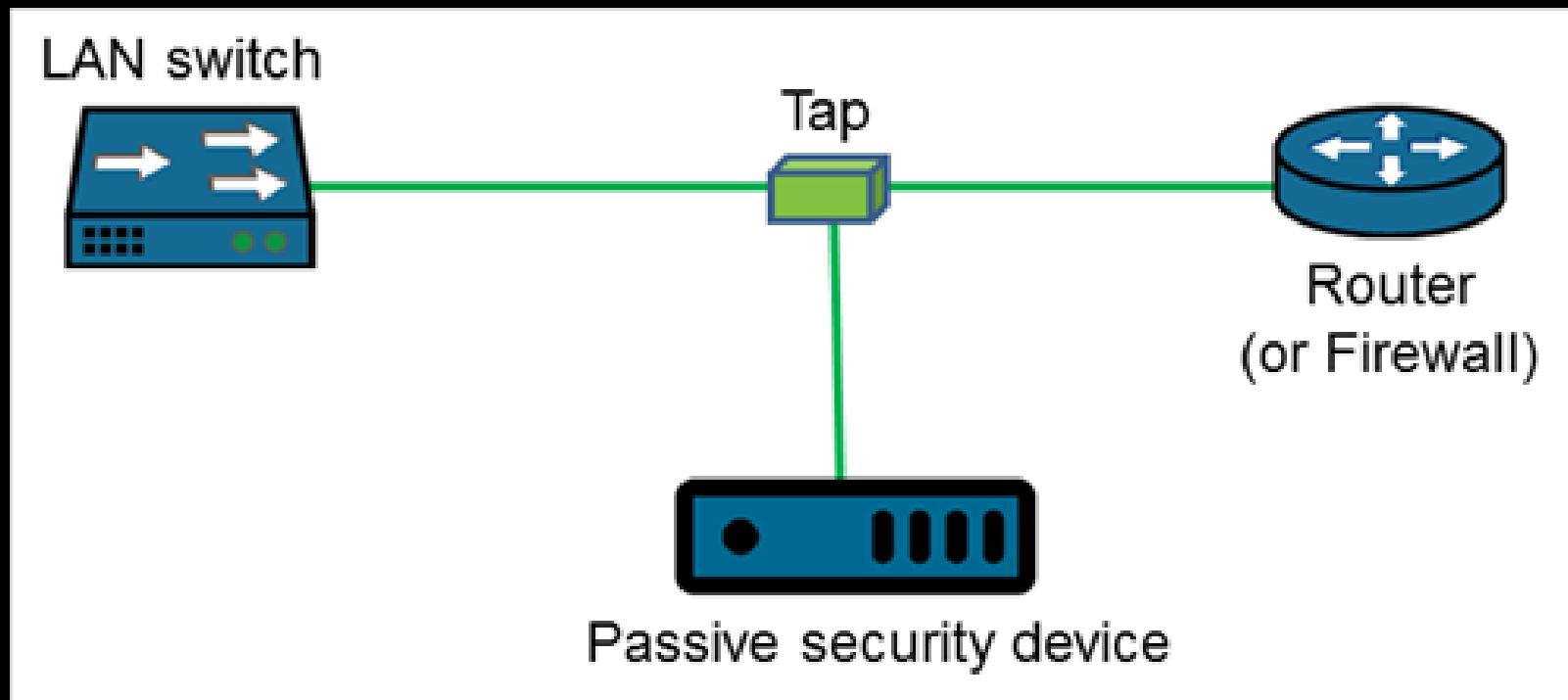
Ubiquiti UniFi US-8

~100 €

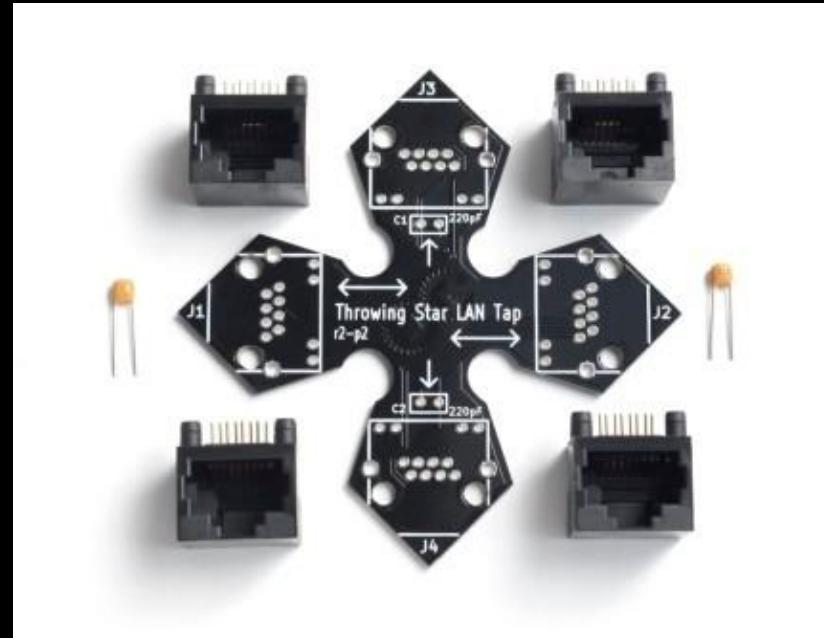
Commutadores de nivel empresarial (Aruba, Cisco, Juniper, etc.)  
> 1000 €

# Grifos Ethernet

Las derivaciones Ethernet son dispositivos pasivos en línea que duplican las tramas Ethernet que pasan por el dispositivo.



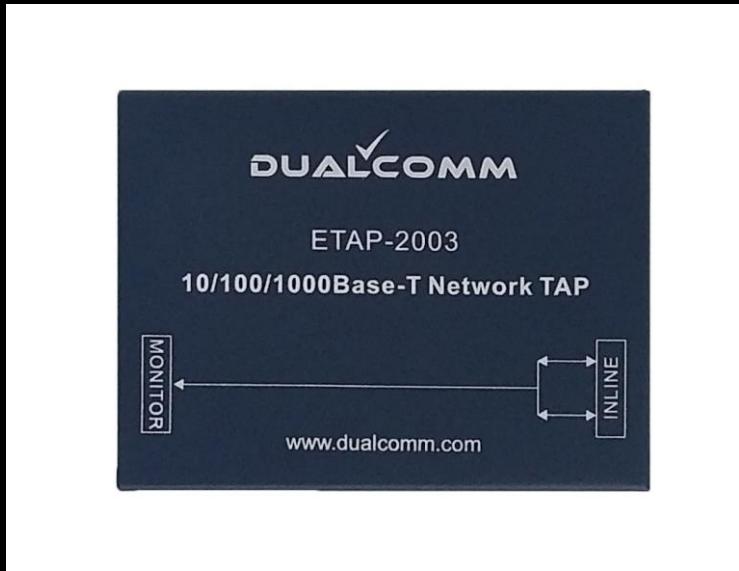
# Ethernet Taps



Throwing Star LAN TAP  
(apto para redes de hasta 100 Mbps)  
40 €

\*Nota - Cada puerto de salida capta tráfico sólo en UNA dirección.

# Ethernet Taps



DualComm ETAP-2003  
10/100/1000Base-T  
~180 €



SharkTap 10/100/1G  
10/100/1000Base-T  
~180 €

# Interfaces de usuario

# squill

SQUILL-0.9.0 – Connected To 192.168.8.250

File    Query    Reports    Sound: Off    ServerName: 192.168.8.250    UserName: bamm    UserID: 2    2014-11-07 02:02:09 GMT

RealTime Events | Escalated Events |

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	fin-ext	1.313990	2014-11-07 00:44:43	222.186.21.55	4270	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	1	fin-ext	1.313991	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
RT	1	fin-ext	1.313992	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious Scan
RT	1	fin-int	7.1033042	2014-11-07 00:50:06	23.235.46.133	80	192.168.8.77	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	1	fin-ext	1.313993	2014-11-07 00:50:06	23.235.46.133	80	97.95.102.96	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	10	fin-int	7.1033043	2014-11-07 00:50:20	192.168.8.77	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	10	fin-ext	1.313994	2014-11-07 00:50:20	97.95.102.96	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	2	fin-int	7.1033052	2014-11-07 00:54:11	192.168.8.77	51775	192.168.8.253	53	17	ET CURRENT_EVENTS DNS Query to a .tk domain – Likely Hostile
RT	18	fin-int	7.1033054	2014-11-07 00:54:12	192.168.8.77	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	18	fin-ext	1.314003	2014-11-07 00:54:12	97.95.102.96	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	16	fin-ext	1.314022	2014-11-07 00:59:23	122.225.109.100	50117	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	16	fin-int	7.1033080	2014-11-07 00:59:23	122.225.109.100	50117	192.168.8.8	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	8	fin-ext	1.314031	2014-11-07 01:03:40	122.225.109.100	34787	97.95.102.96	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	8	fin-int	7.1033089	2014-11-07 01:03:40	122.225.109.100	34787	192.168.8.8	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	1	fin-ext	1.314059	2014-11-07 01:31:02	221.229.162.150	6000	97.95.102.96	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	2	fin-ext	1.314060	2014-11-07 01:40:46	97.95.102.96	44752	192.30.252.129	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	fin-int	7.1033117	2014-11-07 01:41:31	192.168.8.72	64916	192.30.252.131	22	6	ET SCAN Potential SSH Scan OUTBOUND

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs |

Show Packet Data  Show Rule

Reverse DNS  Enable External DNS

Src IP:   
Src Name:

Dst IP:   
Dst Name:

Whois Query:  None  Src IP  Dst IP

% [whois.apnic.net]  
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

% Information related to '122.225.109.0 – 122.225.109.127'

inetnum: 122.225.109.0 – 122.225.109.127  
netname: DINGQI-NETWORK-TECHNOLOGY  
country: CN  
descr: Shaoxing Dingqi Network Technology Co., Ltd.  
descr:  
admin-c: JS2095-AP  
tech-c: CH119-AP  
mnt-irt: IRT-CHINANFT-71

Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum

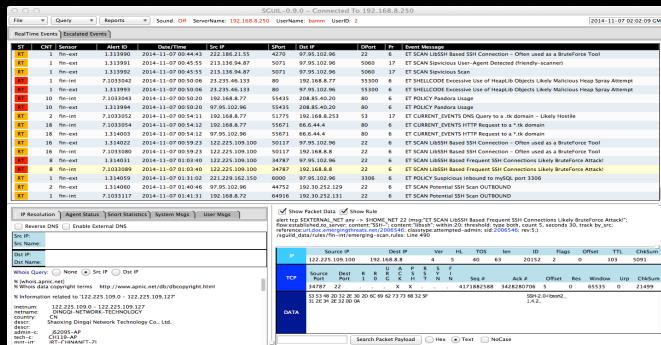
TCP Source Port Dest Port R R U A P R S F  
R Port G K C S S Y I  
H T N N Seq # Ack # Offset Res Window Upd ChkSum

DATA 34787 22 . . X X . . 4171882588 3428280706 5 0 65535 0 21499

53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 32 5F  
31 2E 34 2E 32 0D 0A

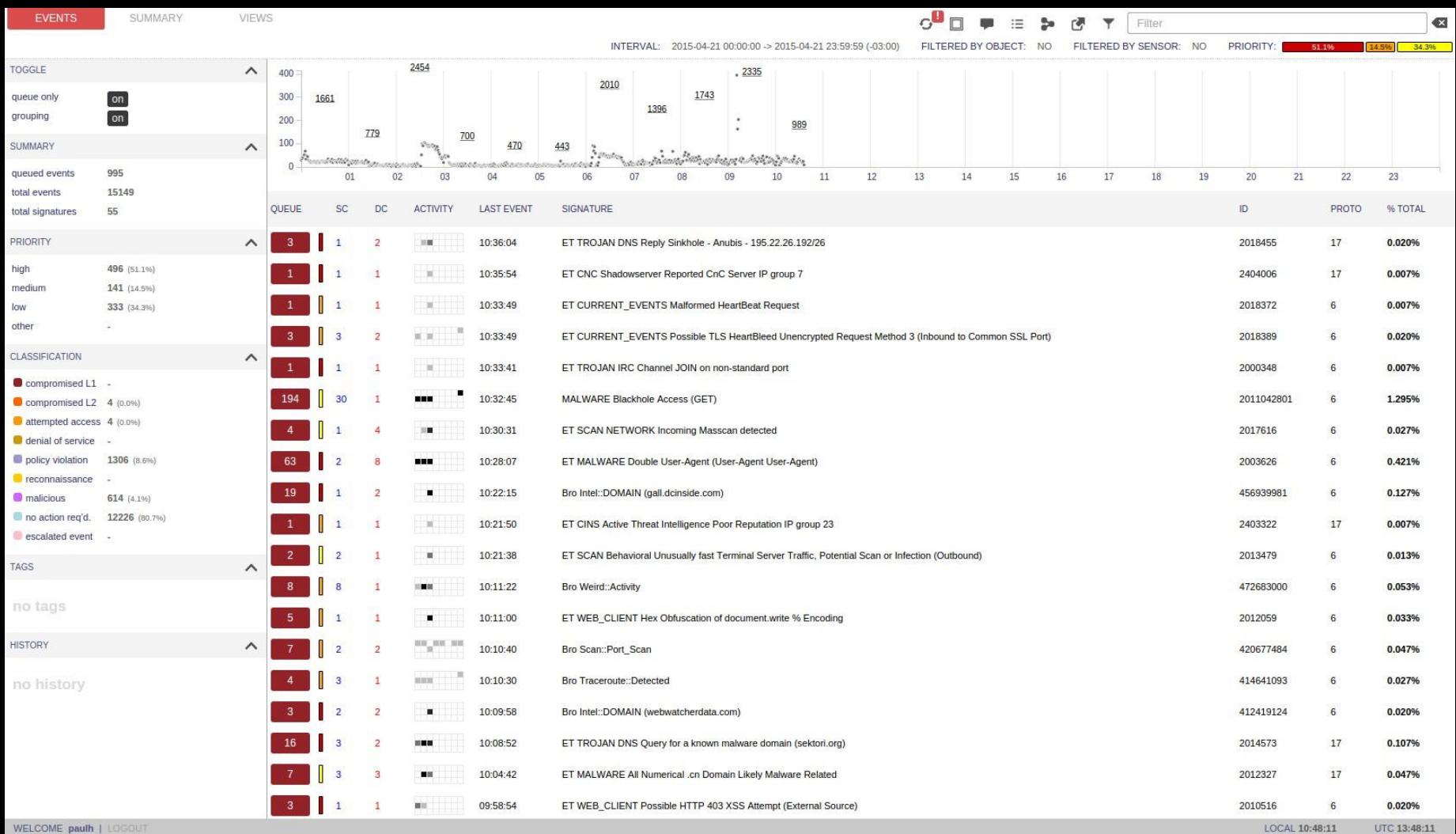
Search Packet Payload  Hex  Text  NoCase

# squil

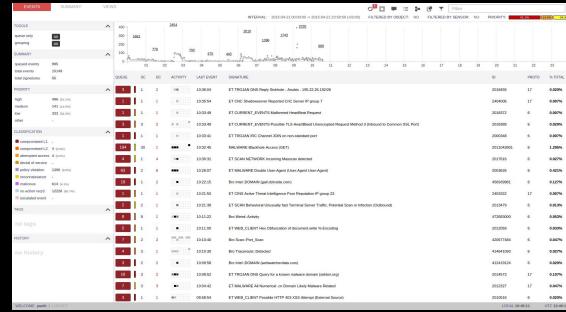


El componente principal de Sguil es una interfaz gráfica de usuario intuitiva que proporciona acceso a eventos en tiempo real, datos de sesión y capturas de paquetes sin procesar. Sguil facilita la práctica de la supervisión de la seguridad de la red y el análisis basado en eventos. El cliente de Sguil está escrito en tcl/tk y puede ejecutarse en cualquier sistema operativo que soporte tcl/tk (incluidos Linux, \*BSD, Solaris, MacOS y Win32).

# squert



# Squert (Simple QUERy and Report Tool)



Squert es una aplicación web que se utiliza para consultar y visualizar datos de eventos almacenados en una base de datos Sguil (normalmente datos de alertas IDS). Squert es una herramienta visual que intenta proporcionar un contexto adicional a los eventos mediante el uso de metadatos, representaciones de series temporales y conjuntos de resultados ponderados y agrupados lógicamente.

# CapMe

**capME!**

Src IP / Port:  /

Dst IP / Port:  /

Start Time:

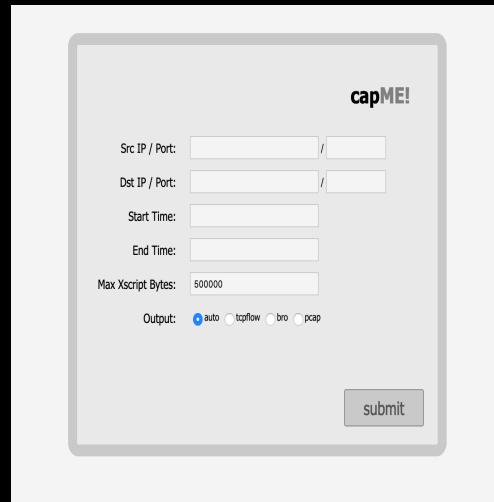
End Time:

Max Xscript Bytes:

Output:  auto  tcpflow  bro  pcap

**submit**

# CapME



**CapME es una interfaz web que le permite:**

- ver una transcripción pcap renderizada con tcpflow
- ver una transcripción pcap renderizada con Bro  
(especialmente útil para tratar con codificación gzip)
- descargar un pcap

# CapMe

[Logout](#)

# Kibana

Noire | Metropolis Record Bro - Connections - Kibana https://10.0.1.10/app/kibana#/dashboard/e0a34b90-34e6-11e7-9118-45bd317f0ca4?\_g=()&\_a=(description:,filters:[{}],fullScreenMode:!t,options:(darkTheme:!t,useMargins:!t),panels:[{}],gridData:!t)

Discover Visualize Dashboard Timelion Dev Tools Management Squert Logout

Bro Hunting Connections DCE/RPC DHCP DNS Files FTP HTTP Intel IRC Kerberos Modbus MySQL NTLM PE RADIUS RDP RFB SIP SMB SMTP SNMP Software SSH SSL Syslog Tunnels Weird X.509 Host Hunting Autorms Beats OSSEC

Discover Visualize Dashboard Timelion Dev Tools Management Squert Logout

Bro Hunting Connections DCE/RPC DHCP DNS Files FTP HTTP Intel IRC Kerberos Modbus MySQL NTLM PE RADIUS RDP RFB SIP SMB SMTP SNMP Software SSH SSL Syslog Tunnels Weird X.509 Host Hunting Autorms Beats OSSEC

Dashboard / Bro - Connections

Add a filter +

Connections - Log Count

138,727

Connections - Log Count Over Time

Count @timestamp per 30 minutes

Connections - Top 10 - Total Bytes By Connection

Connection ID	Total Bytes
C7dKsy4hY5s2BV0Deca	1.304GB
Cq46l14o60argVKMvI	1.118GB
CKzPUPCYdnRvLZTk7	953.674MB
CF97xz36GZ8GQ25Fd	762.939MB
CpaWV3lKQ0PdgRxZ5	572.205MB
CQRlh3u3WGgVPXsoa	381.47MB
Cz4g3036rIm8frMU6	190.735MB
CQadwd1p3MKHU9555	190.735MB
CYQ0Vc1TGYEEU8ABP2	190.735MB
Cqlxrr10dFbiWqFok	190.735MB

Connections - Top 10 - Total Bytes By Destination Port

Destination Port	Total Bytes
443	1.304GB
80	953.674MB
4500	762.939MB
61540	572.205MB
51293	381.47MB
51393	190.735MB
57252	190.735MB
993	190.735MB
22	190.735MB
30840	190.735MB

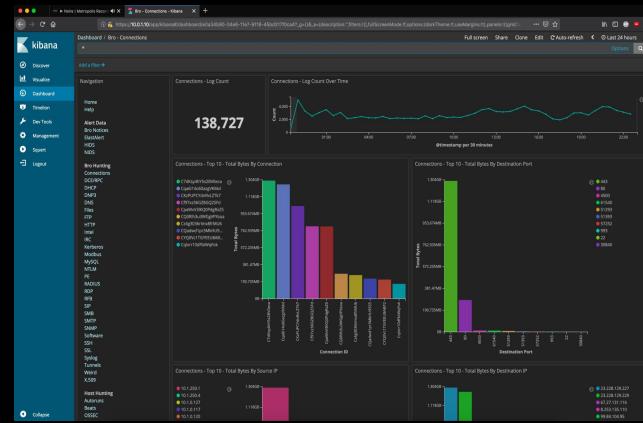
Connections - Top 10 - Total Bytes By Source IP

Source IP	Total Bytes
10.1.250.1	1.304GB
10.1.250.4	1.118GB
10.1.0.127	1.118GB
10.1.0.117	1.118GB
10.1.0.120	1.118GB

Connections - Top 10 - Total Bytes By Destination IP

Destination IP	Total Bytes
23.228.129.227	1.304GB
23.228.129.229	1.118GB
67.27.131.116	1.118GB
8.253.135.110	1.118GB
99.84.104.95	1.118GB

# Kibana



Kibana es una aplicación de frontend gratuita y abierta que se encuentra sobre el Elastic Stack y proporciona capacidades de visualización de datos y de búsqueda para los datos indexados en Elasticsearch. Comúnmente conocida como la herramienta de representación para el Elastic Stack (anteriormente llamado ELK Stack por Elasticsearch, Logstash y Kibana), Kibana también actúa como la interfaz de usuario para monitorear, gestionar y asegurar un cluster del Elastic Stack; además de como concentrador centralizado de las soluciones integradas desarrolladas en el Elastic Stack. Desarrollado en 2013 en la comunidad de Elasticsearch, Kibana ha llegado a ser la ventana al propio Elastic Stack ofreciendo un portal para los usuarios y las empresas.