THE BRIDGE

CYBER SECURITY

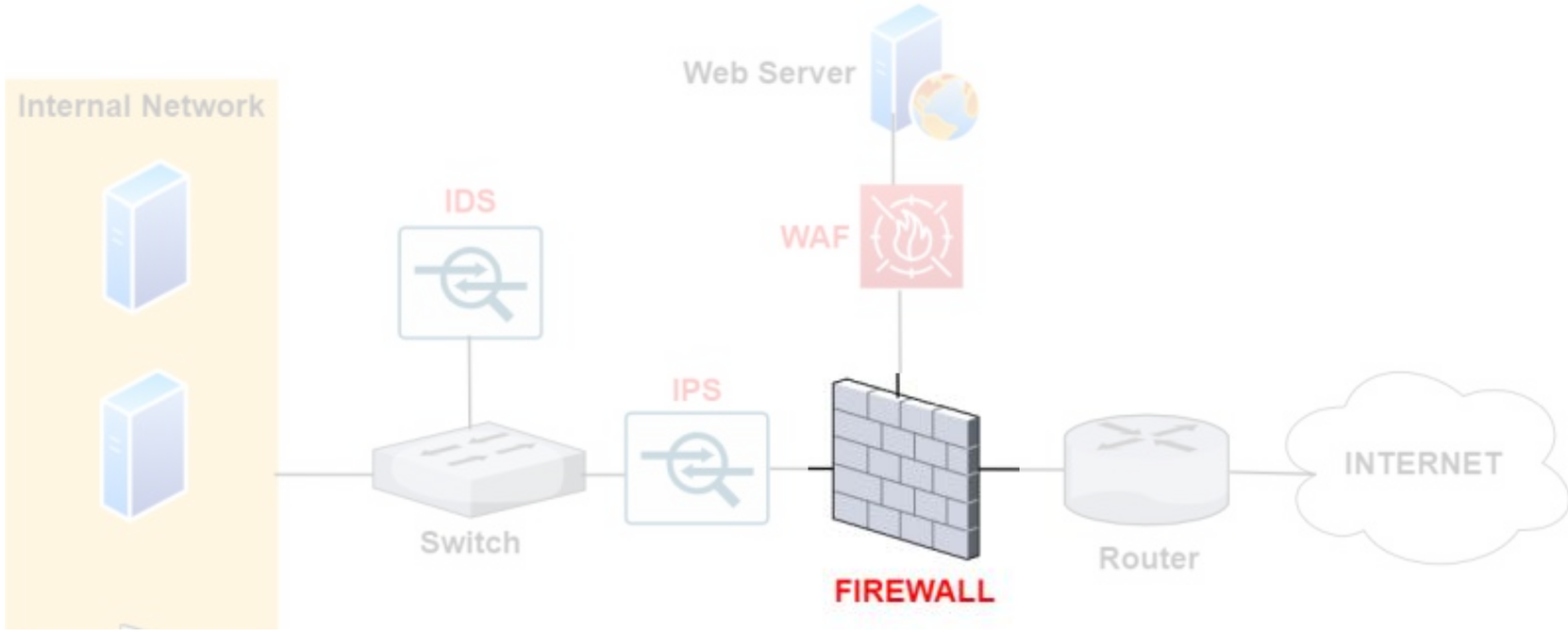
# Protección a la Infraestructuras y redes

# Firewall

- Un **firewall** o **cortafuegos** es un programa o dispositivo de seguridad que protege a una computadora o una red de intrusos. Su función es monitorear y controlar el tráfico de datos entrante y saliente, y bloquear el acceso no permitido o peligroso.

- Los **firewalls** se basan en un conjunto de reglas de seguridad definidas

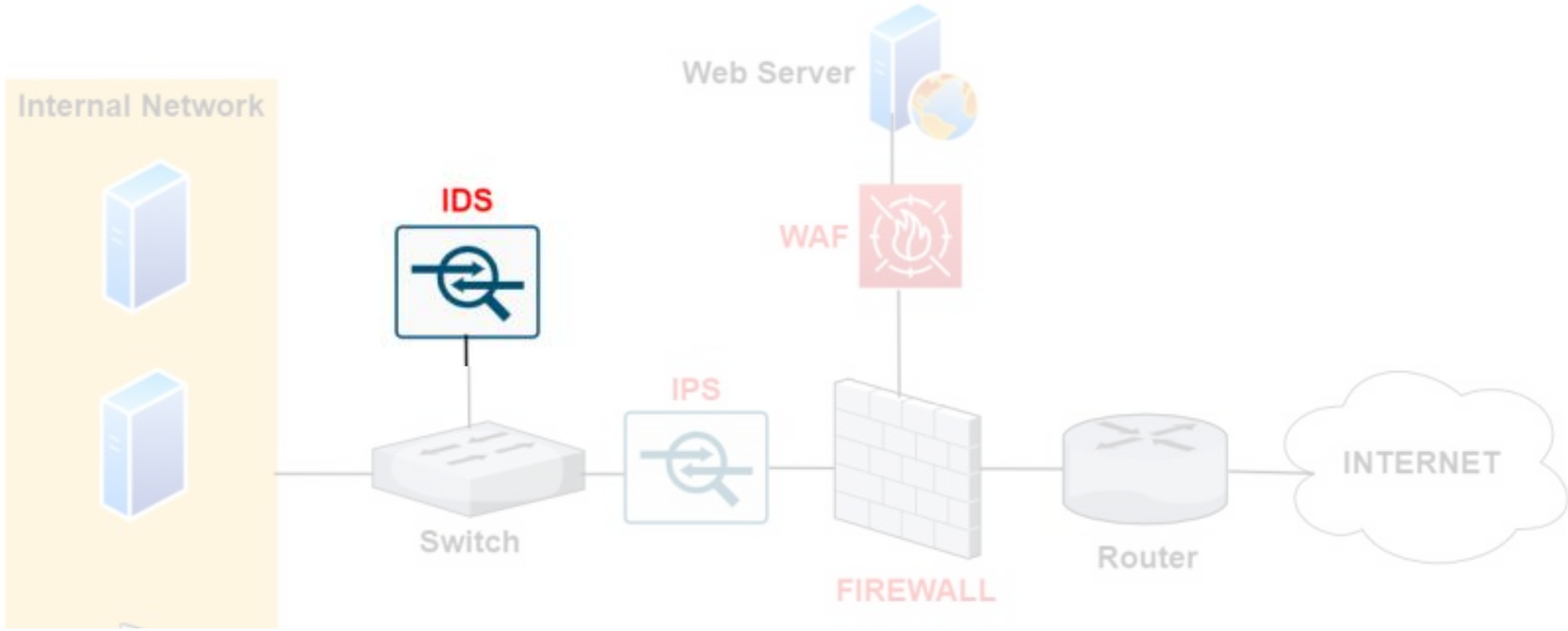
- Pueden funcionar a distintos niveles, siendo los más extendidos:
  - **A nivel de red**: permitiendo o denegando el tráfico en función de la IP de origen y de la IP de destino o a nivel de subredes (conjunto de IPs de origen y de IPs de destino).
  - **A nivel de aplicación**: permitiendo o denegando el tráfico en función del protocolo utilizado en las comunicaciones (p. ej. DNS, NTP…).




https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867

# Sistema de Detección de Intrusiones (IDS)

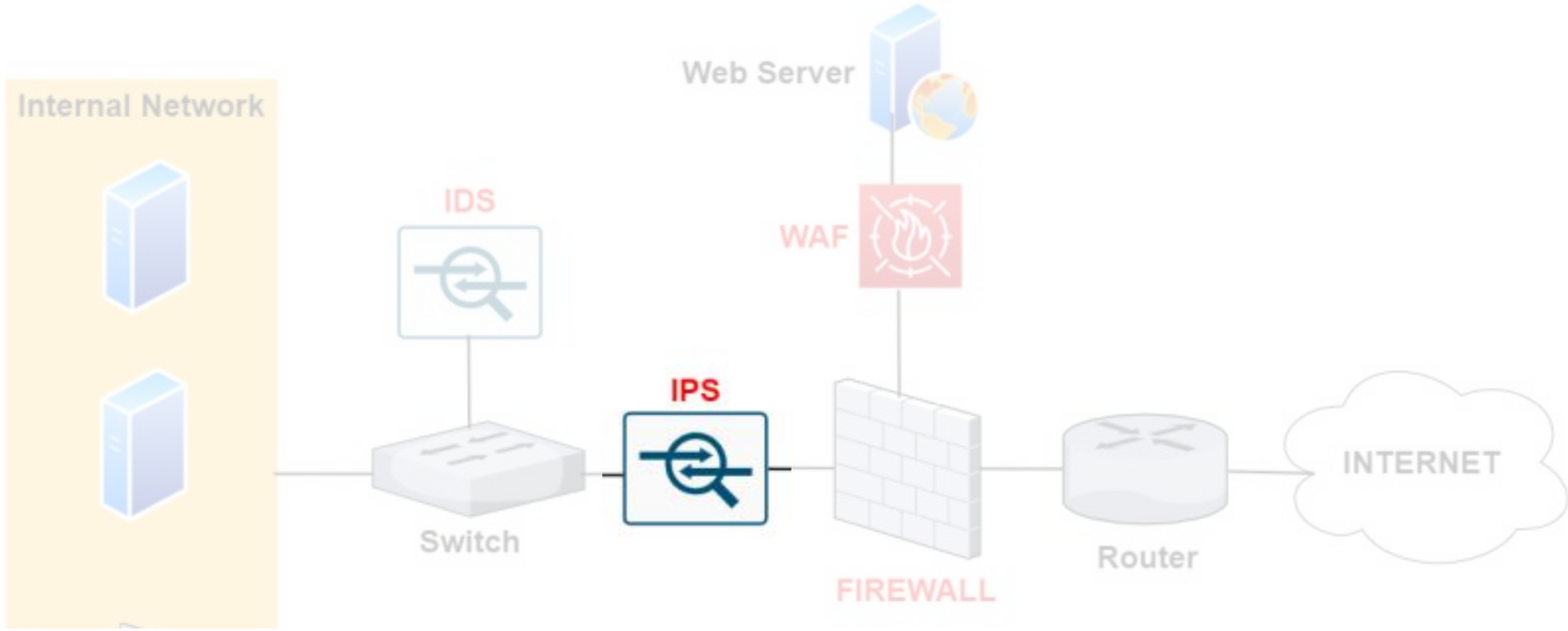
- Un **Sistema de Detección de Intrusiones** (**IDS**) es un software de seguridad que detecta accesos no autorizados en sistemas o redes de computadoras.
- Su función es supervisar el tráfico y los dispositivos de la red en busca de actividades maliciosas conocidas o sospechosas.
- Hay dos métodos principales de detección utilizados por los IDS:
  - **Detección basada en firmas**: Analiza los paquetes de red en busca de firmas de ataques conocidos. Si un paquete coincide con una firma, el IDS lo señala. Sin embargo, esta técnica puede perder nuevos ataques que aún no han sido analizados en busca de firmas.
  - **Detección basada en anomalías**: Utiliza el aprendizaje automático para crear un modelo de referencia de la actividad normal de la red. Luego, compara la actividad real con el modelo y señala desviaciones. Los IDS basados en anomalías pueden detectar ciberataques totalmente nuevos que podrían eludir la detección basada en firmas.




https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867

# Sistema de Prevención de Intrusiones (IPS)

- Un **Sistema de Prevención de Intrusiones** (**IPS**) se encarga de prevenir que los intrusos logren entrar a nuestra red.
- Funciona mediante un conjunto de instrucciones especializadas que monitorean el tráfico de cada bit de datos que ingresa a la red.
- Al detectar amenazas, el IPS toma medidas proactivas, como bloquear el acceso, poner en cuarentena hosts o bloquear sitios web externos que podrían resultar en una filtración de seguridad.
- Los IPS se pueden implementar en el perímetro, el borde empresarial o el centro de datos.
- Utilizan firmas o detección basada en anomalías para identificar tráfico malicioso




https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867

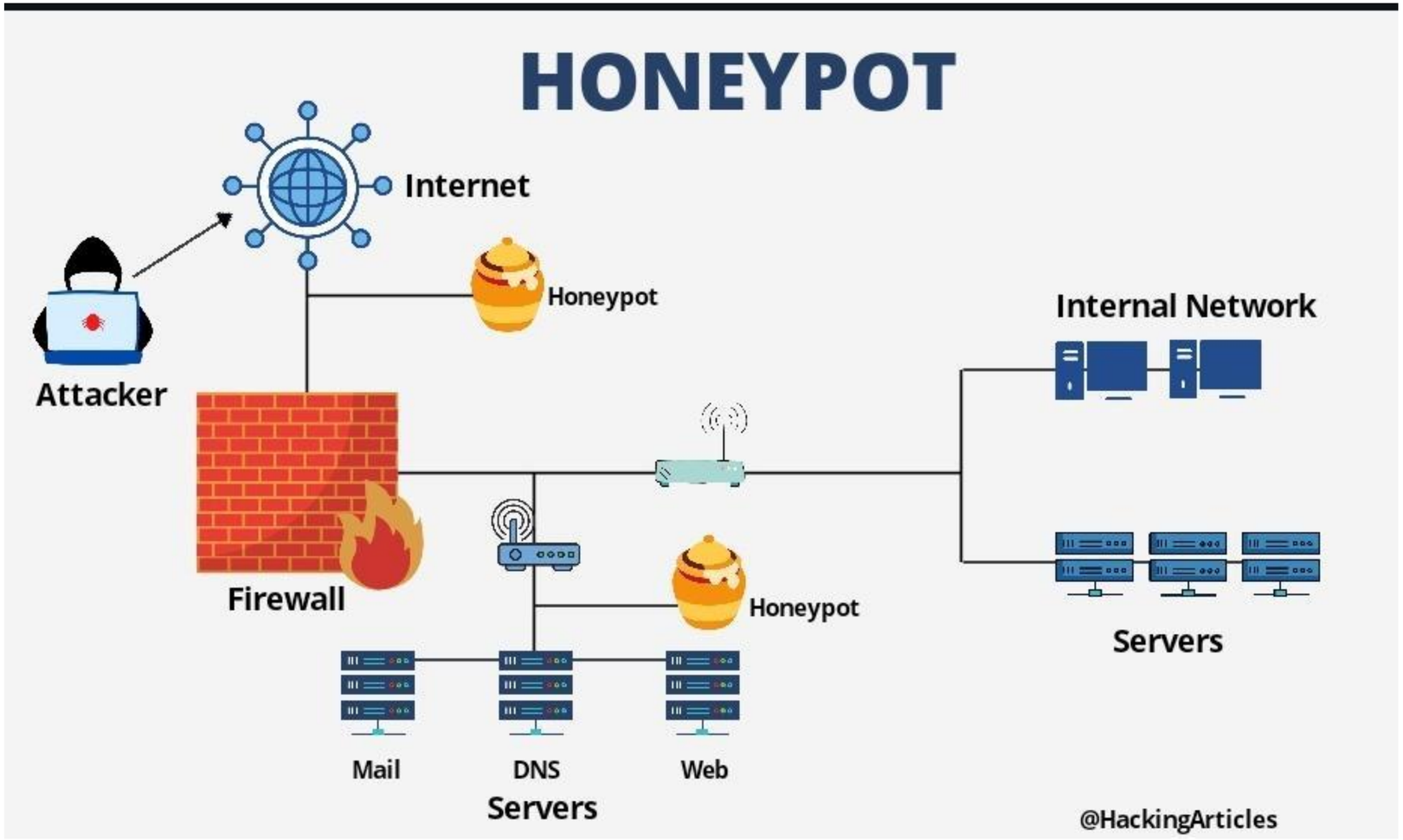
# Honeypots

- Conocido como "**sistema trampa**" o "**señuelo**", es una herramienta de seguridad informática que se coloca en una red o sistema informático con el propósito de atraer posibles ataques.

- Su **objetivo principal** es simular el comportamiento de un sistema real para engañar a los ciber atacantes.

- Estos creen que han accedido a un sistema legítimo y vulnerable, pero en realidad están en un entorno aislado donde los administradores pueden observar sus acciones y las vulnerabilidades que intentan explotar.

- La información recopilada por un **honeypot** es valiosa para las empresas, ya que proporciona detalles sobre las intenciones, comunicaciones y vulnerabilidades utilizadas por los ciberdelincuentes.

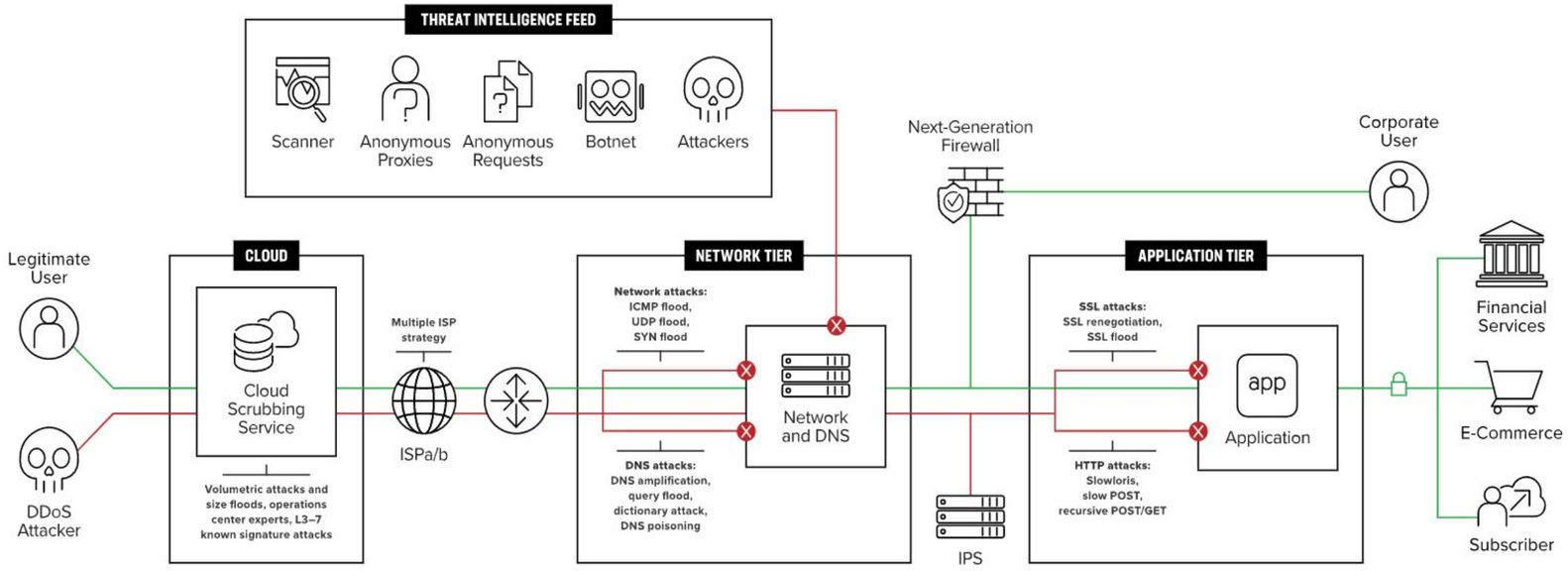



https://www.hackingarticles.in/comprehensive-guide-on-honeypots/

# Anti-DDoS

- Un **sistema anti-DDoS** (**Distributed Denial of Service**) es un conjunto de herramientas y técnicas diseñadas para proteger redes, servidores, aplicaciones y otros recursos de TI contra ataques DDoS.
- Estos ataques buscan interrumpir el servicio normal de un sistema al inundarlo con una cantidad masiva de tráfico falso o malicioso, lo que puede hacer que el sistema se ralentice, se bloquee o quede inaccesible para los usuarios legítimos.
- Aquí hay algunas características y componentes clave de un sistema anti-DDoS:
  1. Monitoreo y Detección
  2. Filtrado de Tráfico
  3. Balanceo de Carga
  4. Rate Limiting
  5. Análisis y Reportes
  6. Escalabilidad:

- El objetivo principal de un sistema anti-DDoS es mantener la disponibilidad y la funcionalidad de los servicios y aplicaciones incluso durante un ataque.
- Estos sistemas son esenciales para las empresas y organizaciones que dependen de la disponibilidad constante de sus recursos en línea.




https://www.f5.com/es_es/solutions/application-security/ddos-protection

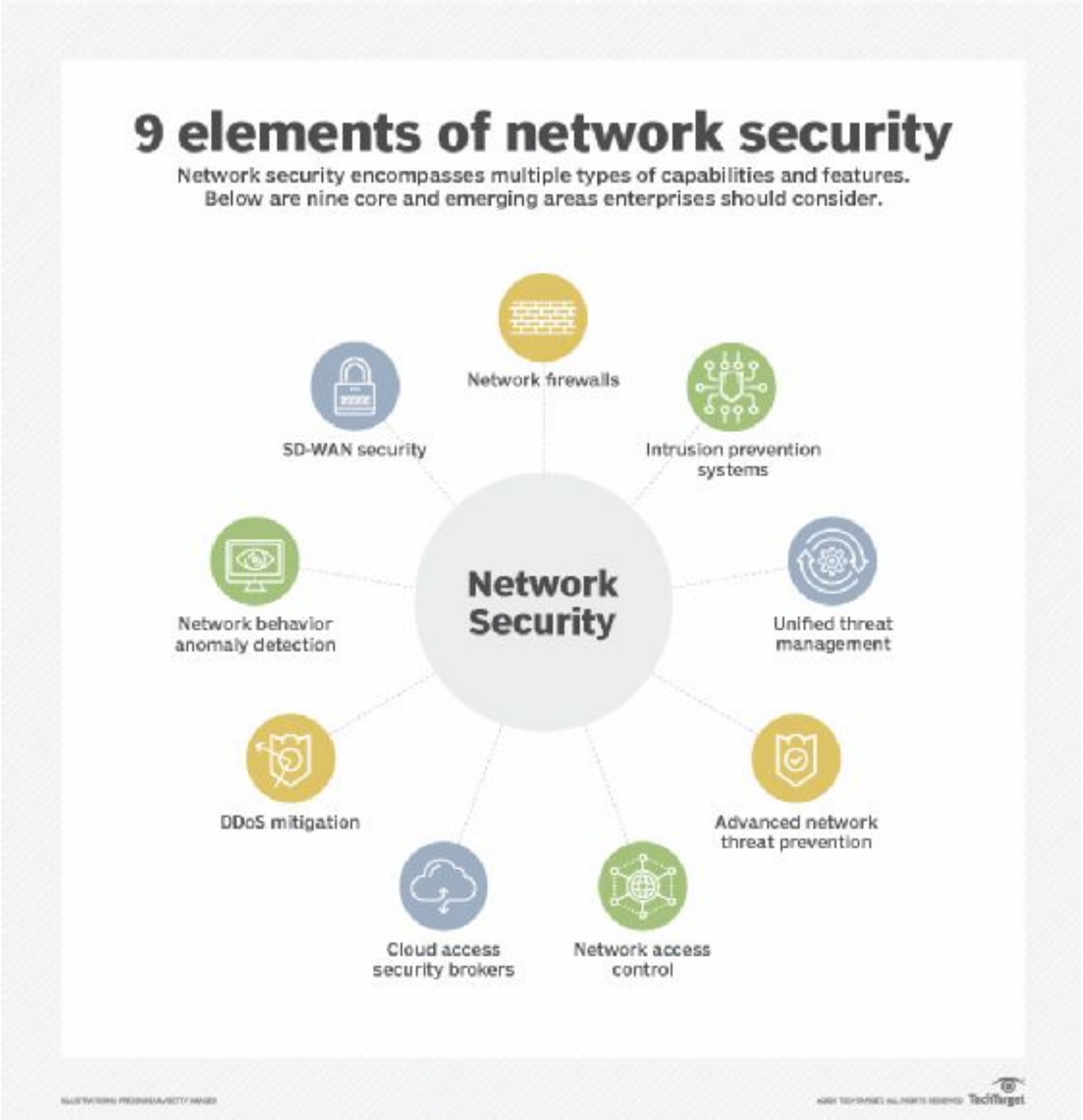
# Control de Accesos a red (NAC)

- Enfoque de seguridad en redes de computadoras que busca unificar tecnologías de seguridad en los dispositivos finales, como antivirus, prevención de intrusiones en hosts y reportes de vulnerabilidades.

- Su objetivo principal es reforzar la seguridad del acceso a la red.

- Las soluciones de **NAC** permiten a las organizaciones restringir el acceso a la red corporativa para dispositivos y usuarios no autorizados o que no cumplen con las políticas de seguridad.

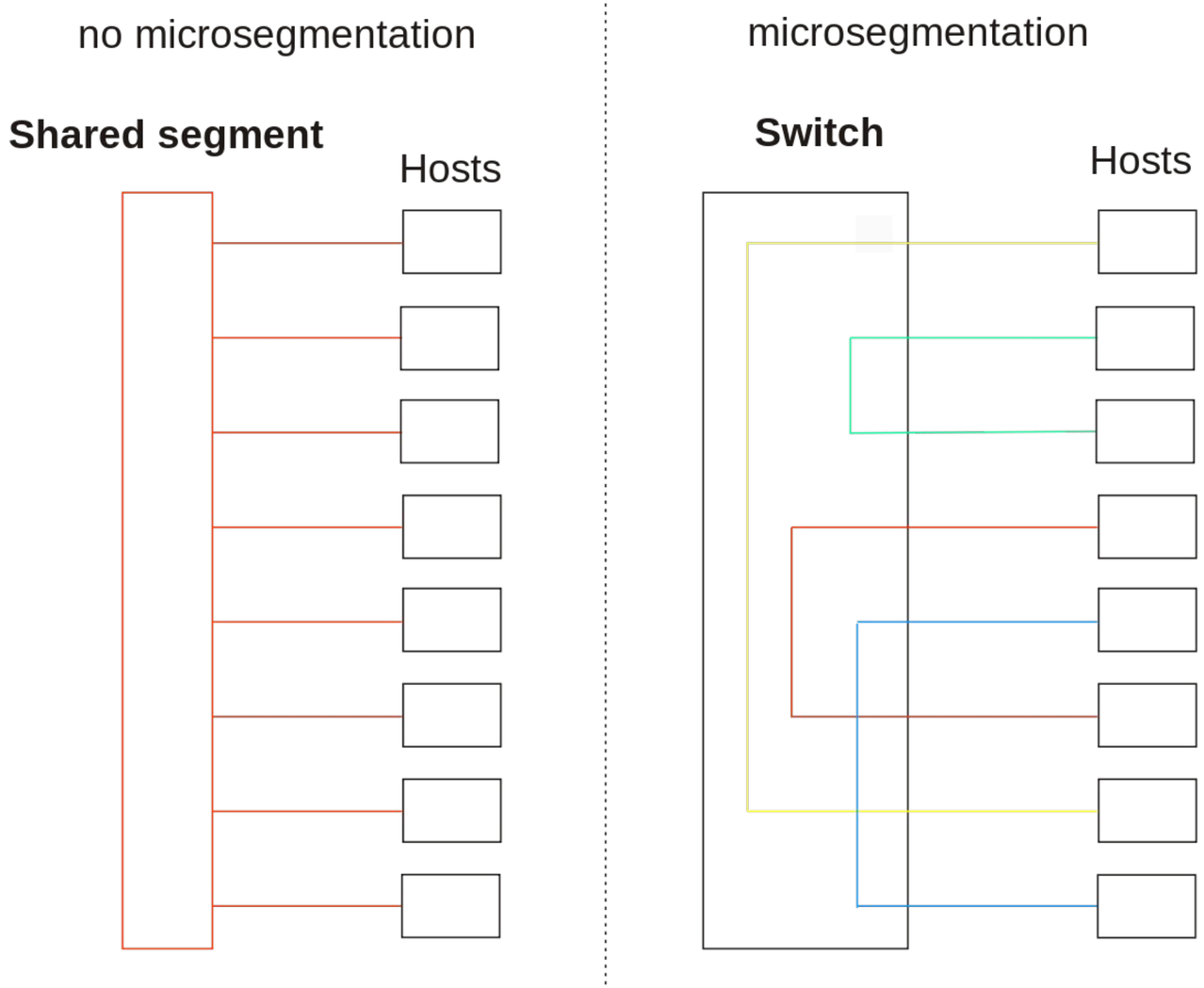
- Las **capacidades generales** de las soluciones de **NAC** incluyen:
  - **Administración del ciclo de vida de la política**
  - **Elaboración de perfiles y visibilidad.**
  - **Acceso a la red para usuarios temporales.**
  - **Comprobación del estado de seguridad.**
  - **Respuesta ante incidentes.**
  - **Integración bidireccional.**




https://www.computerweekly.com/es/definicion/Control-de-acceso-a-la-red-NAC

# Microsegmentación

- La **microsegmentación de redes** es una técnica de seguridad que divide una red en secciones pequeñas y discretas, cada una con sus propias políticas de seguridad y a las que se accede por separado.
- El objetivo principal de la **microsegmentación** es aumentar la seguridad al confinar las amenazas y las fugas al segmento en riesgo sin afectar al resto de la red
- La microsegmentación aplica a cada miembro una política única y centralizada de la red.
- La microsegmentación es necesaria debido a la adopción creciente de servicios en la nube, que van más allá del perímetro de una red tradicional




https://es.wikipedia.org/wiki/Microsegmentaci%C3%B3n

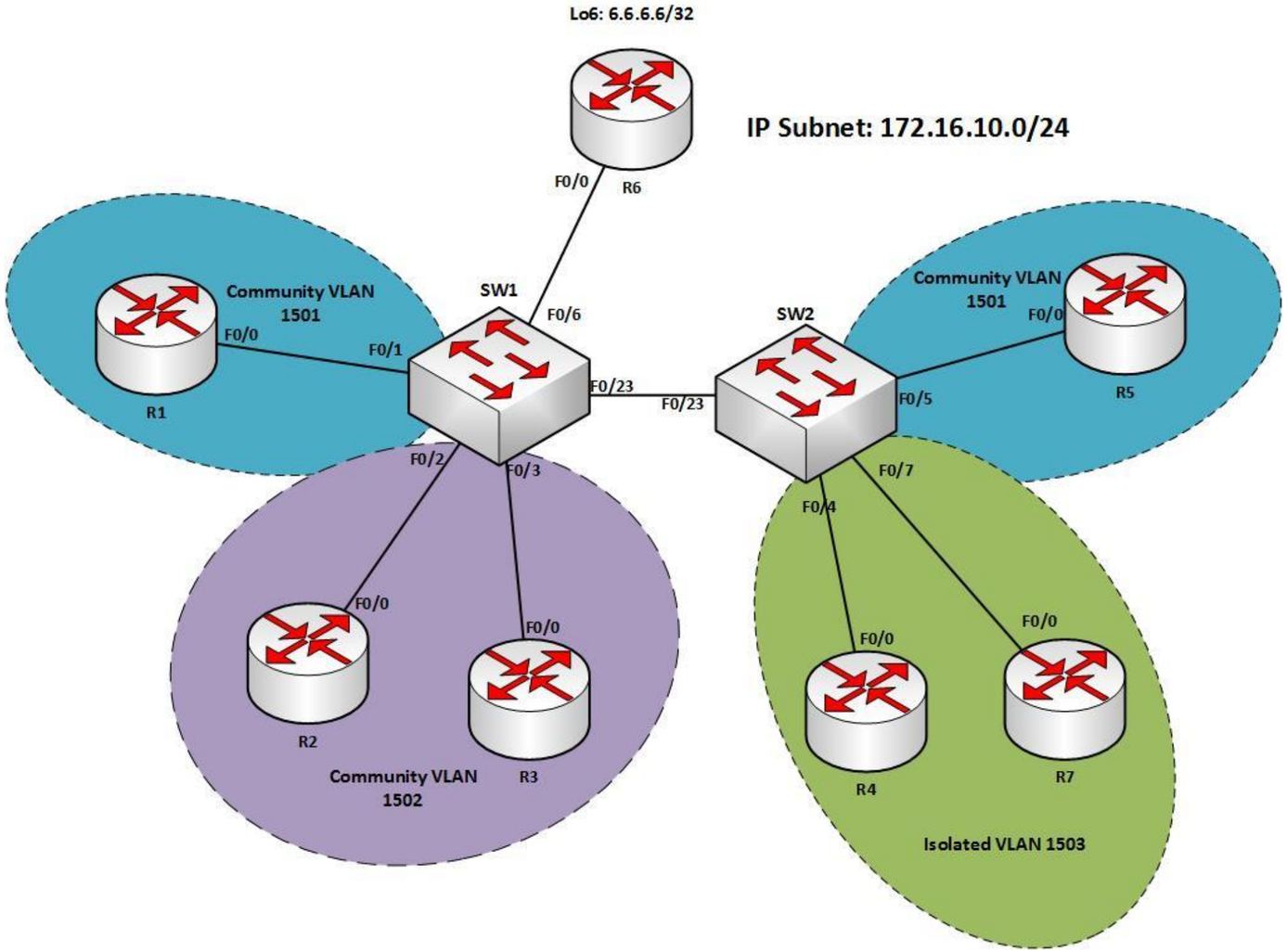
# VLAN

- Las **VLANs** (Virtual LAN), también conocidas como redes de área local virtuales, son una tecnología de redes que nos permite crear redes lógicamente independientes dentro de la misma red física.

- Se usan switches gestionables que soportan **VLANs**, podemos segmentar adecuadamente la red y asignar diferentes subredes a cada **VLAN**.

- Las VLAN permiten crear redes lógicamente independientes, lo que significa que podemos aislarlas para que solo tengan conexión a Internet y denegar el tráfico entre diferentes **VLAN**.

- Por defecto, las VLAN no pueden intercambiar tráfico entre sí. Para habilitar la comunicación entre **VLAN**, necesitamos un dispositivo de nivel 3 (como un **router** o **switch multicapa**) para activar el enrutamiento entre **VLANs**.



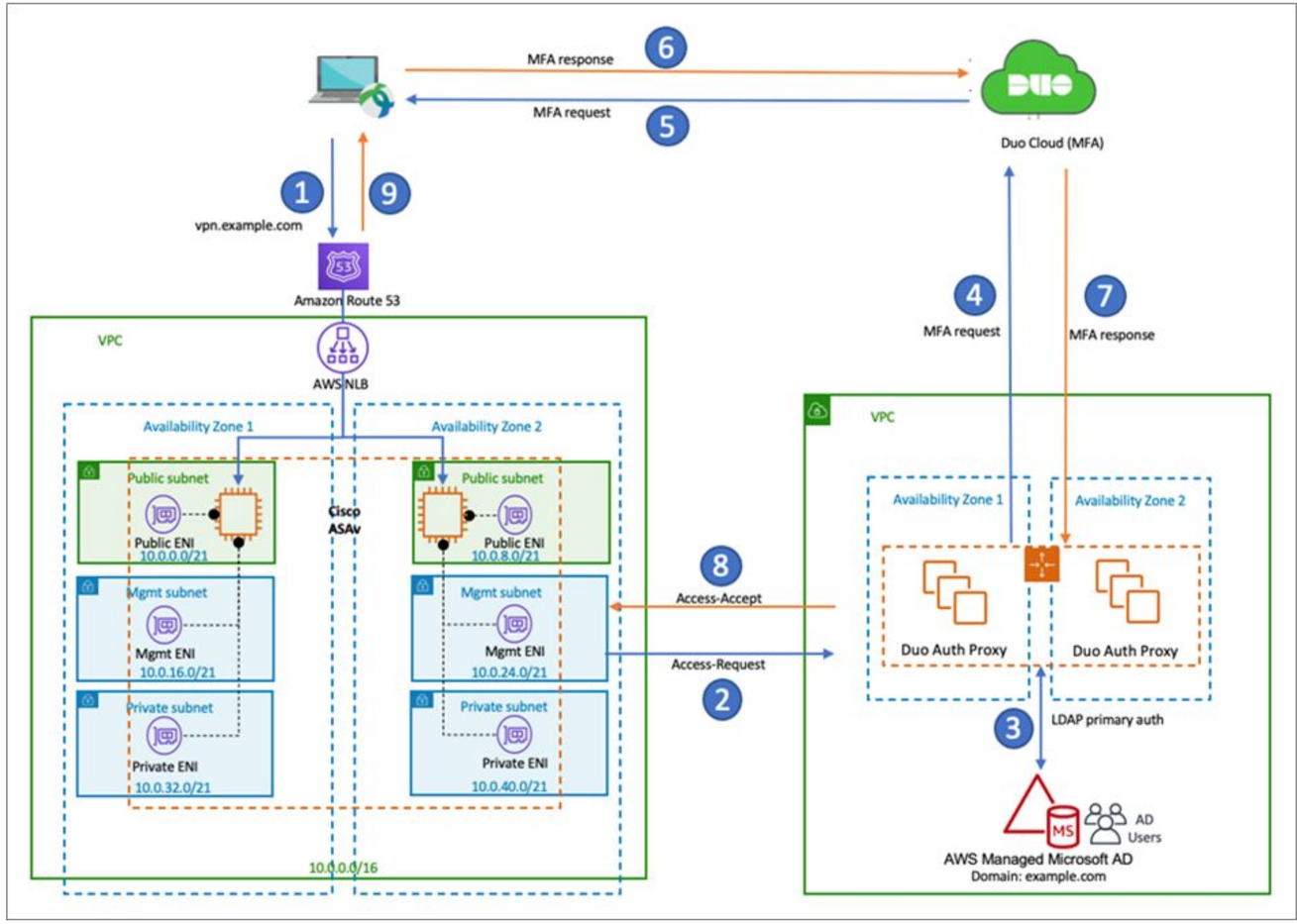

https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKIvEAO/understanding-private-vlans

# VPN

- Una **VPN (Virtual Private Network o Red Privada Virtual**) es una tecnología que permite establecer una conexión segura y cifrada a través de una red pública, como Internet.

- Esta conexión asegura que los datos transmitidos entre el usuario y el servidor **VPN** permanezcan privados y protegidos de posibles interceptaciones o accesos no autorizados.

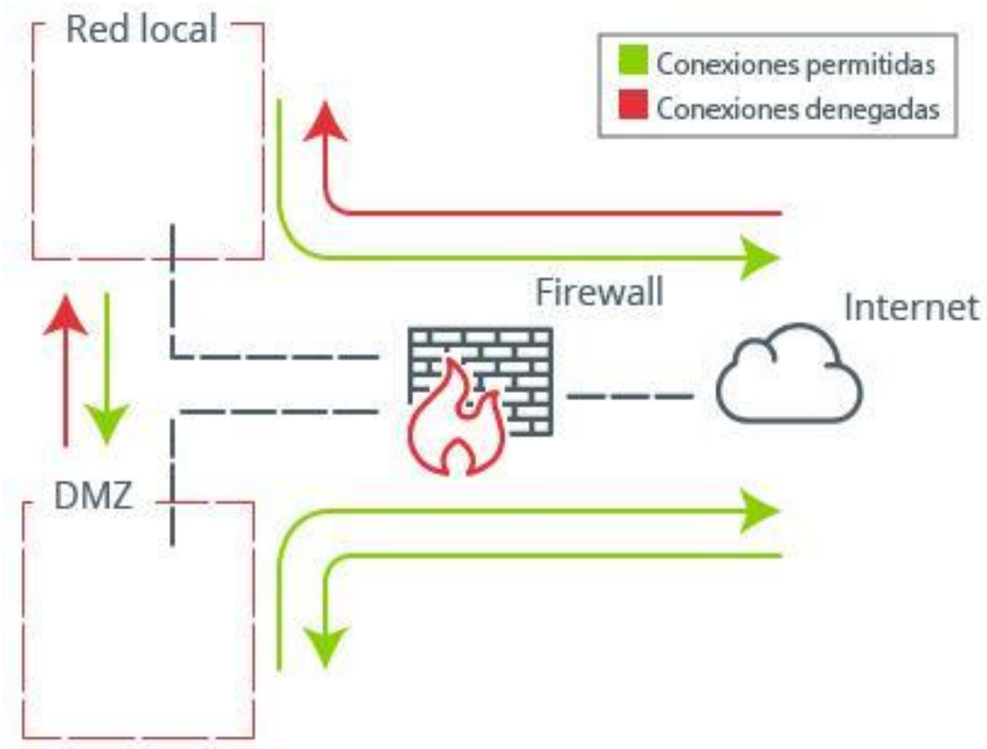
- Características Principales de una **VPN**
  1. **Cifrado de Datos**
  2. **Anonimato**
  3. **Acceso Remoto Seguro**
  4. **Evasión de Restricciones Geográficas**
  5. **Integridad de Datos.**




https://d2908q01vomqb2.cloudfront.net/77de68daecd823babbb58edb1c8e14d7106e83bb/2021/07/22/Cisco-ASAv-VPN-1.png

# DMZ

- Una **DMZ** es una subred que se encuentra entre la Internet pública y las redes privadas de una organización.
- Su objetivo principal es permitir que la organización acceda a redes no confiables (como Internet) mientras mantiene segura su red privada o LAN.
- En la **DMZ**, se almacenan servicios y recursos externos, como servidores para DNS, FTP, correo, VoIP y servidores web. Estos servidores están aislados y tienen acceso limitado a la LAN interna.
- La **DMZ** agrega una capa adicional de seguridad al filtrar el tráfico mediante firewalls.




| Origen | Destino | Política |
|---|---|---|
| Internet | DMZ | Permitido |
| Internet | LAN | Denegado |
| DMZ | Internet | Permitido |
| DMZ | LAN | Denegado |
| LAN | DMZ | Permitido |
| LAN | Internet | Permitido |

https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

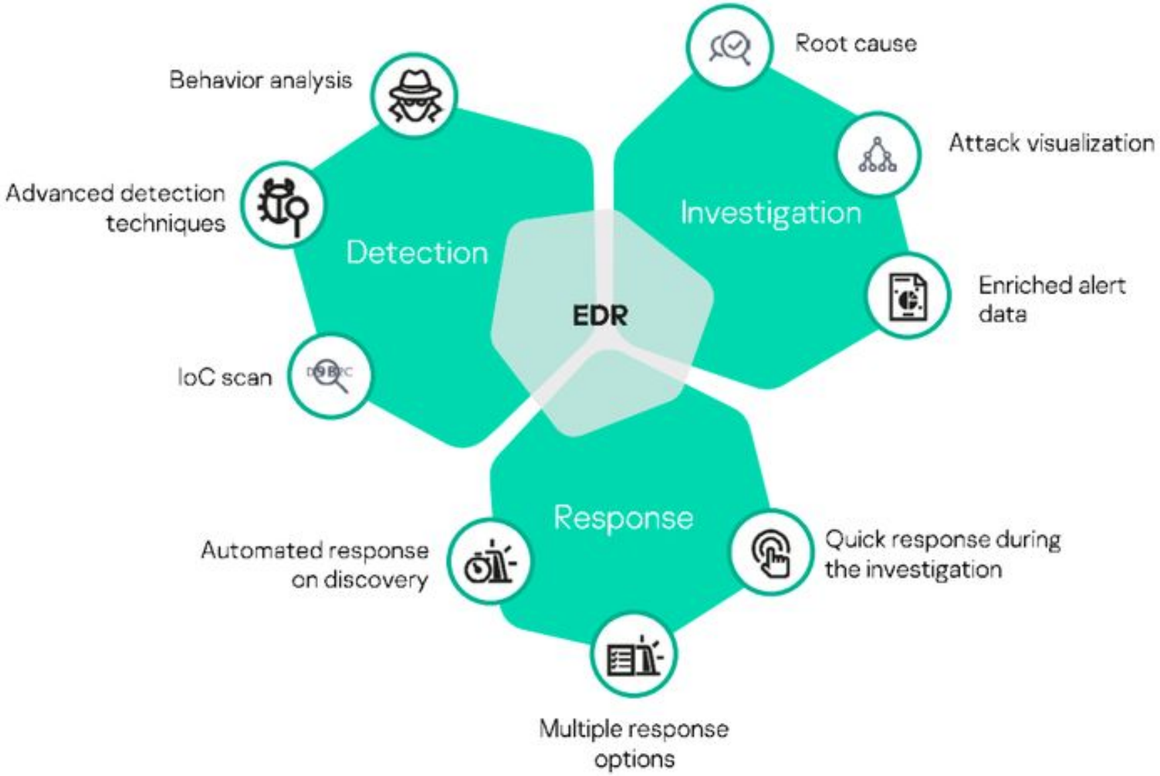
# EDR (Endpoint Detection and Response)

- Un **EDR** (**Endpoint Detection and Response**) es una solución de seguridad diseñada para monitorear y responder a amenazas en los dispositivos finales de una red, como computadoras portátiles, de escritorio y servidores.

- Se enfoca en la detección avanzada de amenazas, la respuesta rápida a incidentes y la remediación de estos.

- Estas soluciones son cruciales para proteger los endpoints contra una amplia gama de amenazas, incluyendo malware, ataques de día cero, y actividades maliciosas avanzadas.

- **Características Principales de un EDR**
  - Monitoreo Continuo.
  - Detección de Amenazas.
  - Respuesta Automática.
  - Investigación y Análisis.
  - Remediación y Contención.
  - Integración con SIEM y SOAR.




https://integracion.cube.net.ar/blog/que-es-edr

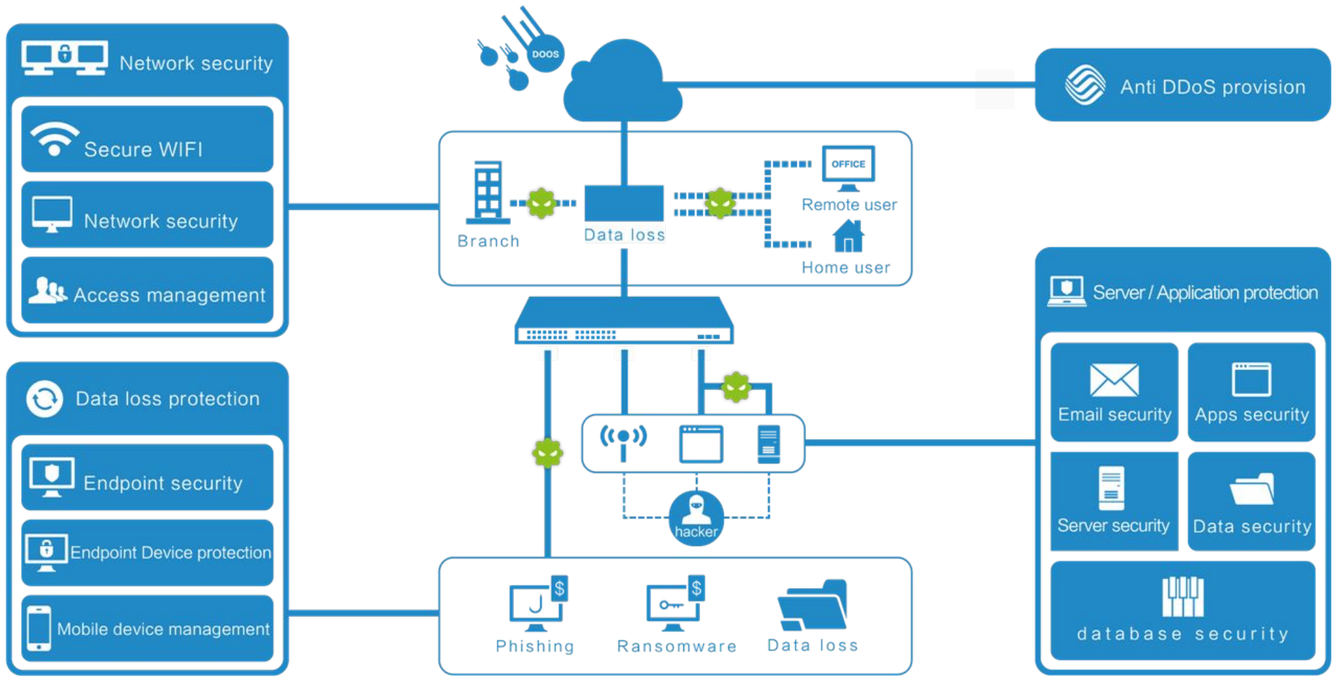
# Seguridad Perimetral

- La seguridad perimetral en el contexto de la seguridad informática se refiere a las medidas y estrategias implementadas para proteger el perímetro de una red corporativa o de una organización.

- El "perímetro" es la frontera entre la red interna segura y el mundo exterior no confiable, generalmente representado por Internet.

- El objetivo principal de la seguridad perimetral es prevenir el acceso no autorizado, detectar amenazas potenciales y proteger los datos y sistemas críticos de la organización.

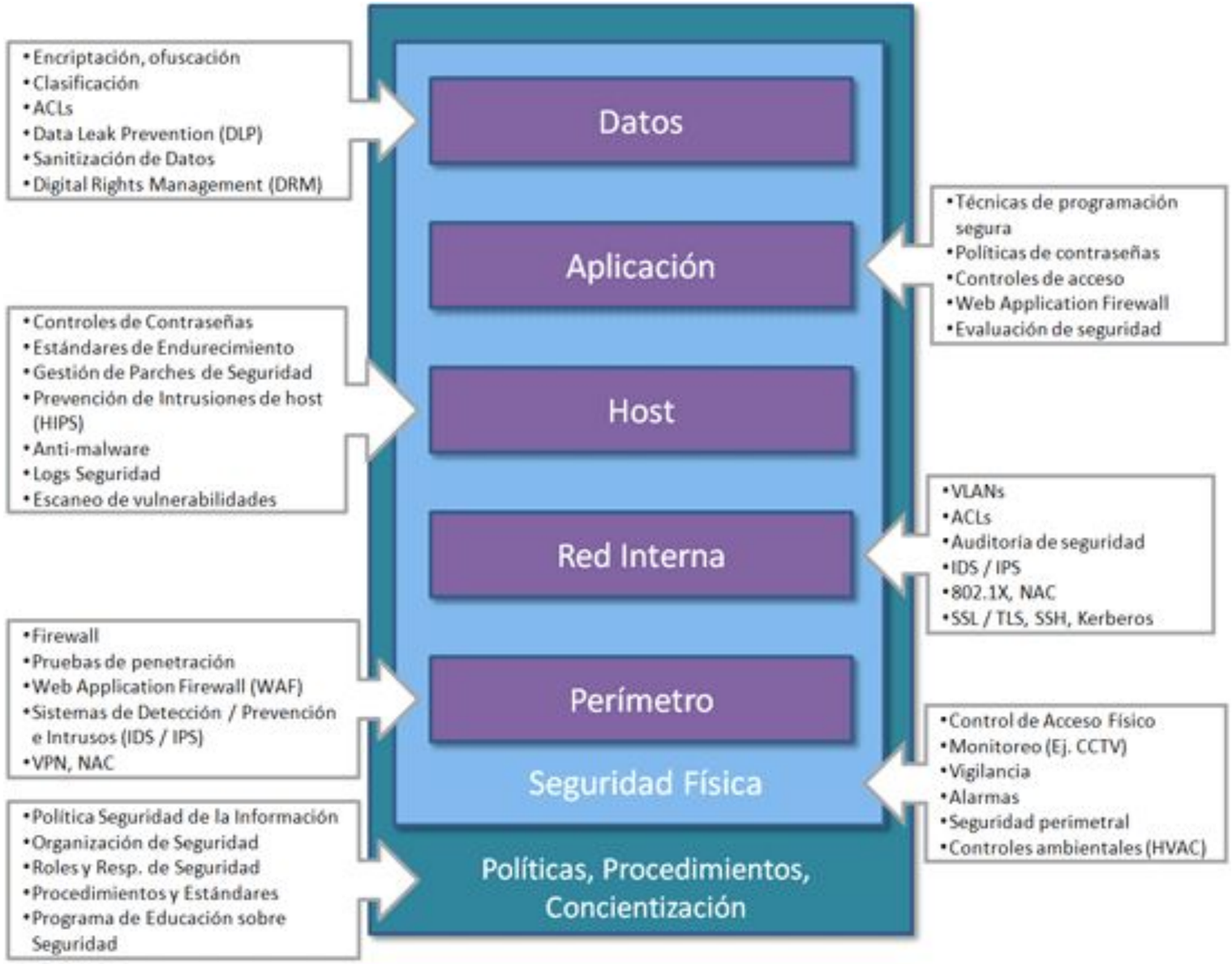
- Algunos Componentes Clave de la Seguridad Perimetral
  - Firewalls
  - Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)
  - Redes Privadas Virtuales (VPN)
  - Gateways de Seguridad de Email y Web
  - Sistemas de Control de Acceso
  - Proxies y Gateways de Contenido
  - Sistemas de Gestión Unificada de Amenazas (UTM)




https://www.iicybersecurity.com/seguridad-logica-seguridad-perimetral.html

# Defensa en Profundidad

- También llamado **Defense in Depth**.
- Se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas.
- La idea de este modelo es muy sencilla: si es posible proteger a un activo de la organización con más de una medida de seguridad, hágalo.
- El objetivo del modelo también es claro: para que un atacante llegue a un dato o información, debe poder vulnerar más de una medida de seguridad**.**
- Aquí están los aspectos clave de la defensa en profundidad:
  - **Capa física:** Protege el acceso físico a los sistemas y dispositivos.
  - **Capa administrativa:** Incluye políticas, procedimientos y capacitación para el personal.
  - **Capa técnica:** Utiliza herramientas y tecnologías como cortafuegos, antivirus y análisis de comportamiento.




https://gallegobeltran.wordpress.com/2014/02/28/4-seguridad-informatica-tema/

# Zero Trust

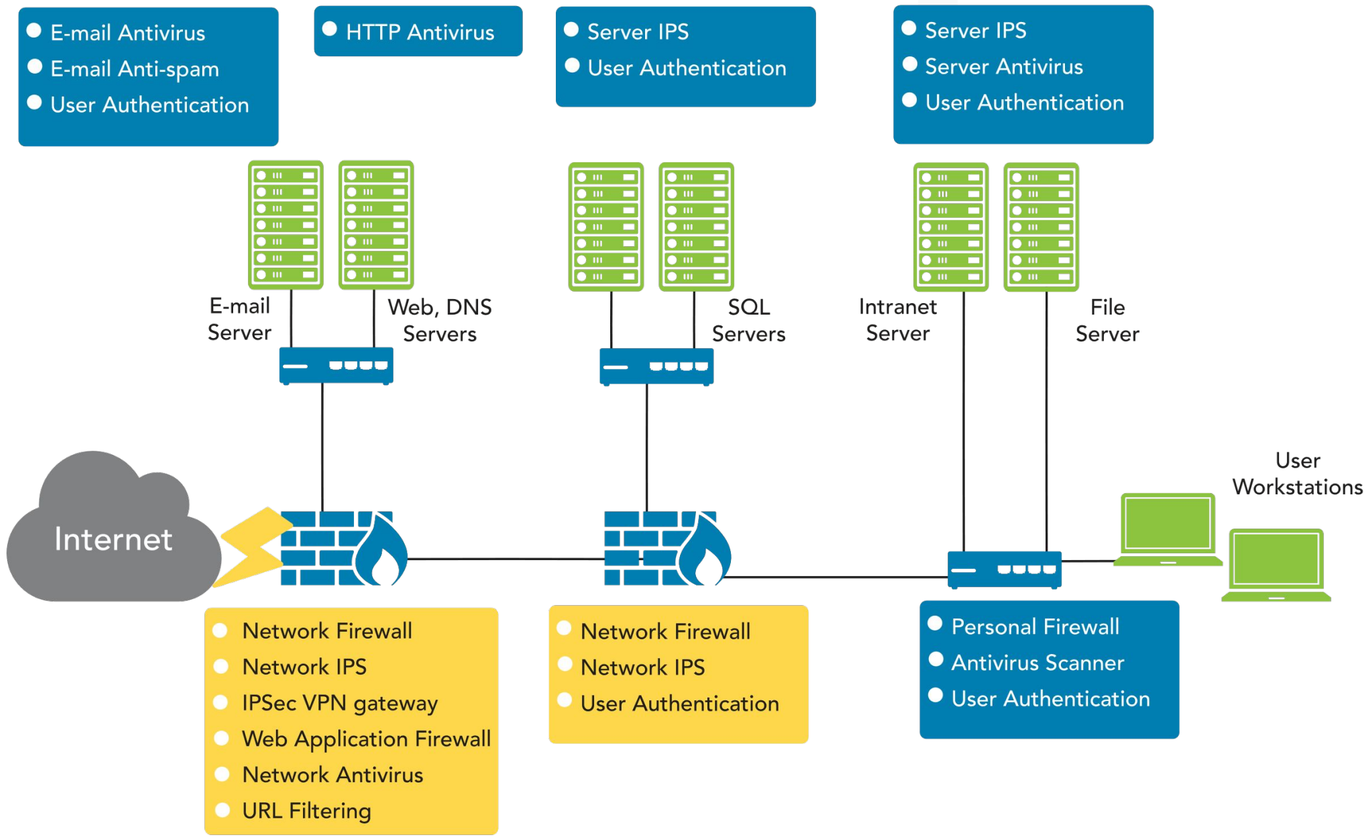
- Modelo de seguridad de la información que **no confía implícitamente en nada** dentro o fuera de su perímetro de red.

- En lugar de eso, requiere **autenticación** o **verificación** antes de otorgar acceso a datos confidenciales o recursos protegidos.

- Este enfoque se basa en la premisa de **"nunca confíes, verifica siempre"**.

- **Principios de Zero Trust:**
  - **Cada usuario, dispositivo y conexión debe ser verificado antes de acceder a recursos.**
  - **Registro e inspección de todo el tráfico.**
  - **Control de acceso limitado.**
  - **Protege los recursos de la red y verifica cada transacción individual**.

- **Beneficios de Zero Trust:**
  - **Adaptabilidad y continuidad**.
  - **Gestión proactiva de amenazas**.
  - **Seguridad basada en datos.**




THE
BRIDGE