THE BRIDGE

CYBER SECURITY

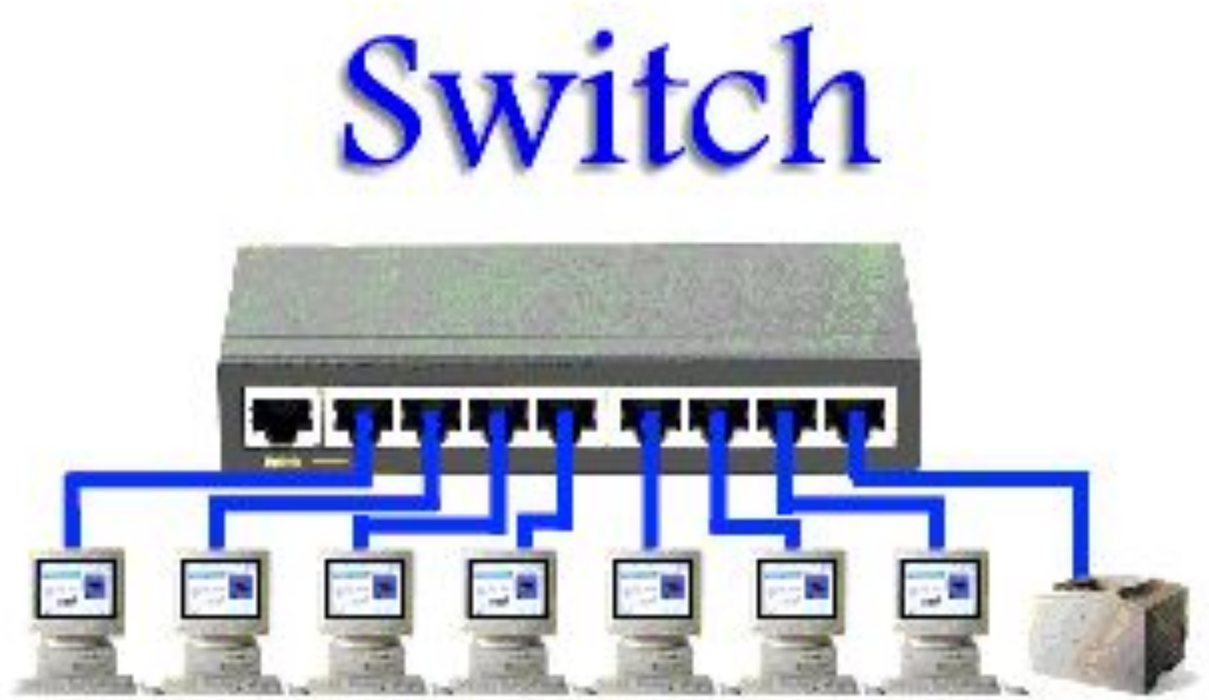
Fundamento de Redes II

Hardware de Red

- Un **concentrador**, también conocido como **Hub**, es un dispositivo de red que permite centralizar diferentes nodos de una red de computadoras.
- Su función principal, establecer una conexión entre un número indefinido de computadoras y permitir el intercambio de datos.
- En cuanto al modelo **OSI**, actúan en la **capa física (capa 1).**

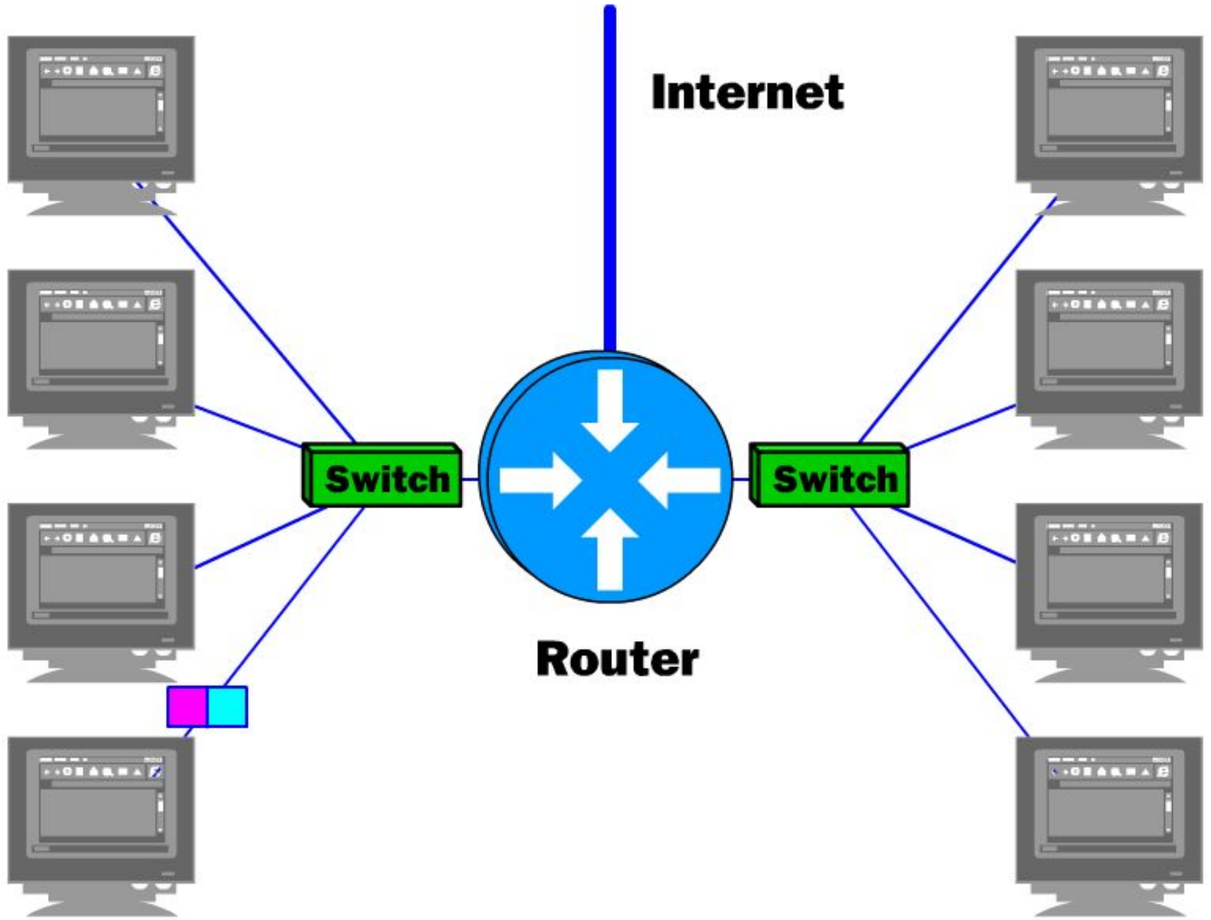
Hardware de Red

- Un **Switch** de red es un dispositivo de **Capa 2** que transmite la información a través de cables en una red.
- Tiene cualquier número de puertos en la parte delantera para las conexiones físicas de dicha red.
- Normalmente, son puertos RJ45 para cables Ethernet.
- El número de puertos puede variar. Hay Switches de red con 4 puertos, 8 puertos,... hasta incluso 96 puertos.



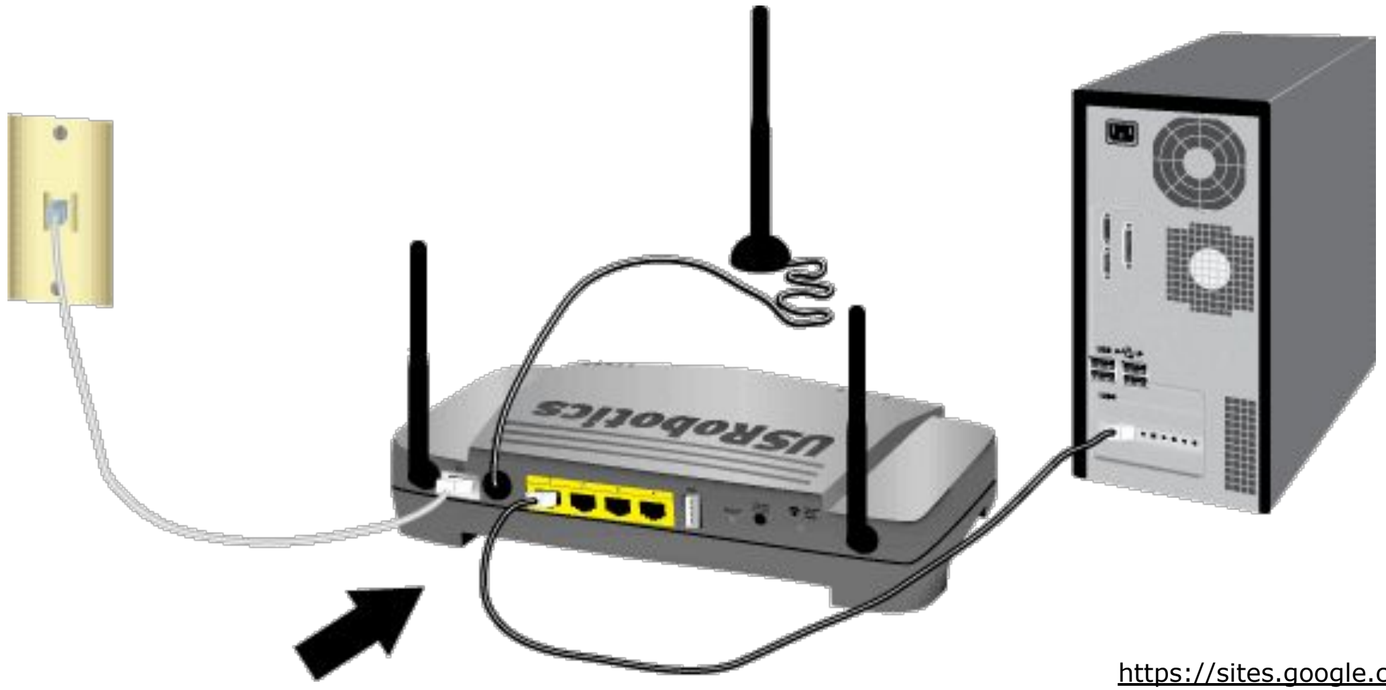
Hardware de Red

- Un **rúter**, enrutador (del inglés **router**) o encaminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP.
- Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.
- Es bastante utilizado para conectarse a Internet ya que conecta la red de nuestro hogar, oficina o cualquier red a la red de nuestro proveedor de este servicio.



Puerta de enlace

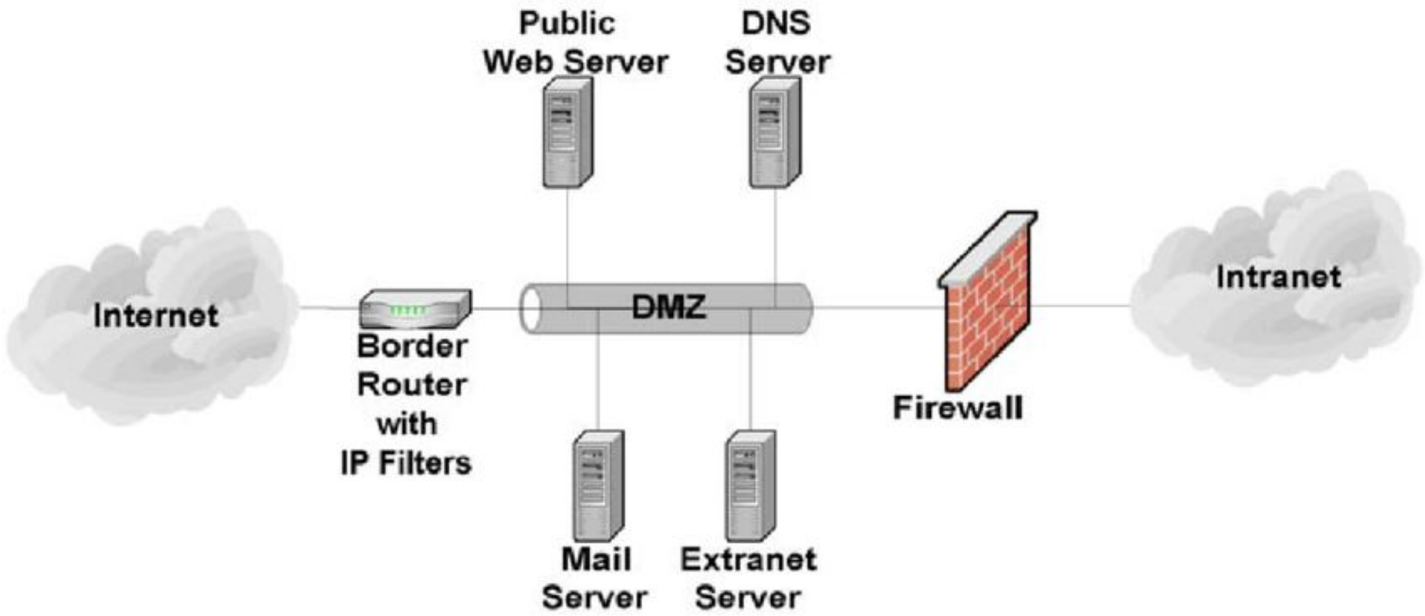
- La **puerta de enlace**, también conocida como **Gateway**
- Es un dispositivo que actúa como interfaz de conexión entre diferentes aparatos o dispositivos en una red.
- Su función principal es traducir la información del protocolo utilizado en una red inicial al protocolo utilizado en la red de destino. En otras palabras, sirve de enlace entre dos redes, permitiendo el acceso desde una red a otra.
- Un ejemplo común de puerta de enlace es un **Router.** Cuando un dispositivo se conecta a un **Router**, este se convierte en la puerta de enlace para ese dispositivo, facilitando la comunicación entre las redes.



https://sites.google.com/site/desireycristinaies/enrutamiento-o-puerta-de-enlace

DMZ

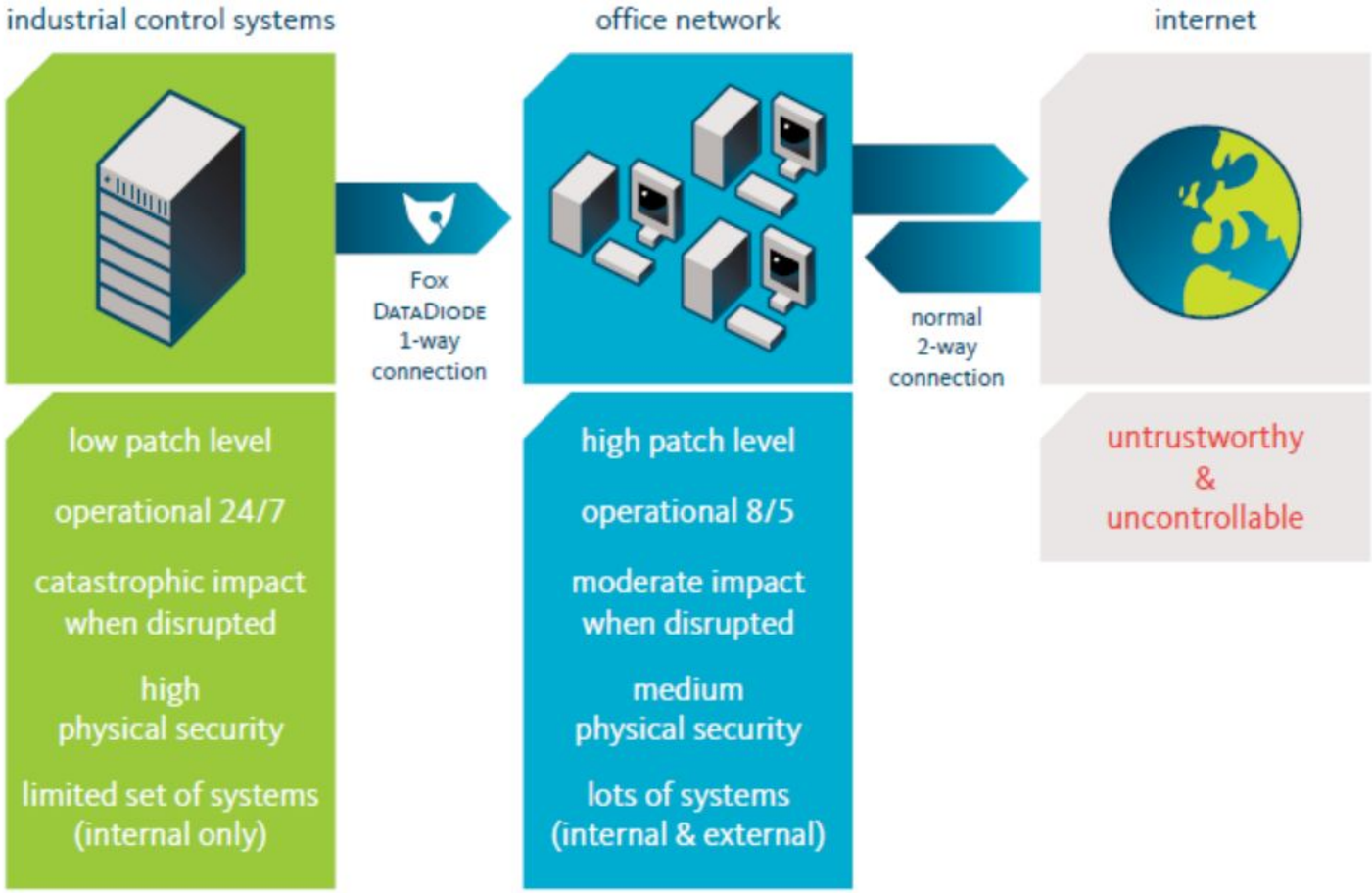
- Acrónimo de "**zona desmilitarizada**" en español, es una subred que se encuentra entre la red interna de una organización y la red externa, generalmente Internet.
- Esta capa intermedia de protección se utiliza para aislar los sistemas críticos de la red interna de la organización de posibles amenazas externas.
- Se expone servicios externos a redes no confiables y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en redes internas.
- Las organizaciones suelen alojar servidores y recursos externos, como servidores web, DNS, FTP, correo, proxy y VoIP.
- Estos servidores están aislados y tienen acceso limitado a la LAN interna, lo que dificulta que un atacante obtenga acceso directo a los datos de la organización y a los servidores internos a través de Internet.



https://www.researchgate.net/figure/Simple-Single-Firewall-DMZ_fig3_330026401

Diodo de Datos

- Es un **Hardware**, no existe software.
- Asegura la **Unidireccionalidad** de las comunicaciones.
- Esto se usa para reemplazar la zona **DMZ** (ZONA DESMILITARIZADA)
- Se utiliza para proteger redes que maneja datos sensibles o que sean muy vulnerables y estas no se puedan modificar sus componentes.
- Una vez que ha sido desplegado, no se requiere una gestión y un mantenimiento exhaustivo como en el caso de los firewalls
- El principal inconveniente es que, si se requieren escenarios bidireccionales, el diodo no debería plantearse inicialmente como opción
- Se utiliza en equipos industriales (OT), Banca y defensa principalmente.



https://www.ciberseguridadlogitek.com/microsite/documentos/ciberseguridadlogitek_DataDiode_FoxIT_wp.pdf

VPN

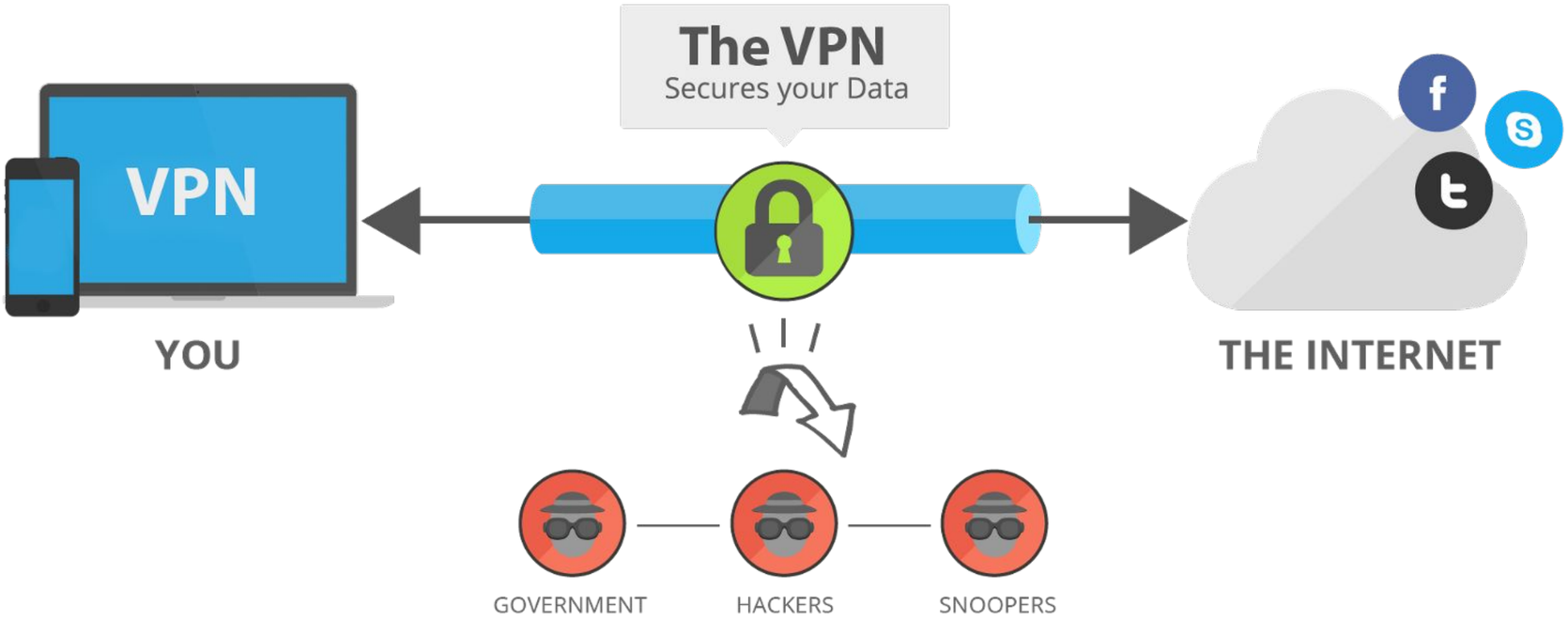
- Una **VPN** (**Red Privada Virtual, por sus siglas en inglés**) es una herramienta digital que crea una conexión segura entre tu dispositivo e Internet.

- Aquí tienes algunas características clave:

  - **Privacidad y seguridad**: Cifra tu tráfico en Internet, lo que dificulta a terceros rastrear tus actividades en línea o robar tus datos.

  - **Protección en redes públicas**: Cuando te conectas a una red Wi-Fi pública, una VPN protege tus datos al cifrar la comunicación entre tu dispositivo y el servidor al que te conectas.

  - **Anonimato parcial**: Aunque no proporciona un anonimato completo, una VPN oculta tu dirección IP y dificulta que tu proveedor de Internet sepa a qué te dedicas en línea.



https://web-tech.fr/quelle-est-la-difference-entre-un-vpn-et-un-proxy/

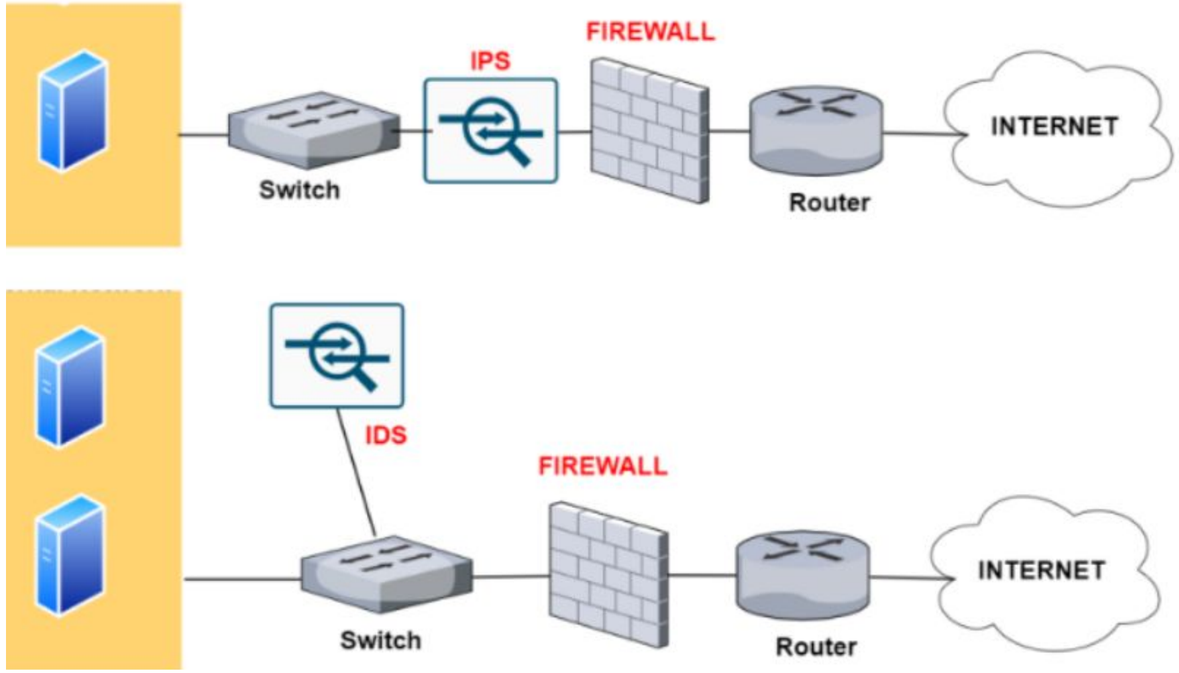
Hardware de Red

- **Firewall**
  - Un cortafuegos (del término original en inglés firewall) está diseñada para bloquear el acceso no autorizado usando reglas.
  - Puede ser de Hardware o Software
  - Se usan para separar y seguridad en las redes.

- **IDS**: Un sistema de detección de intrusos (Intrusion Detection System) es un sistema de supervisión que detecta actividades sospechosas y genera alertas al detectarlas.

- **IPS**: Los sistemas de prevención de intrusiones (Intrusion Prevention System) detectan o previenen los intentos de explotar las debilidades en sistemas o aplicaciones vulnerables, protegiéndolo en la carrera por explotar la última amenaza de ruptura

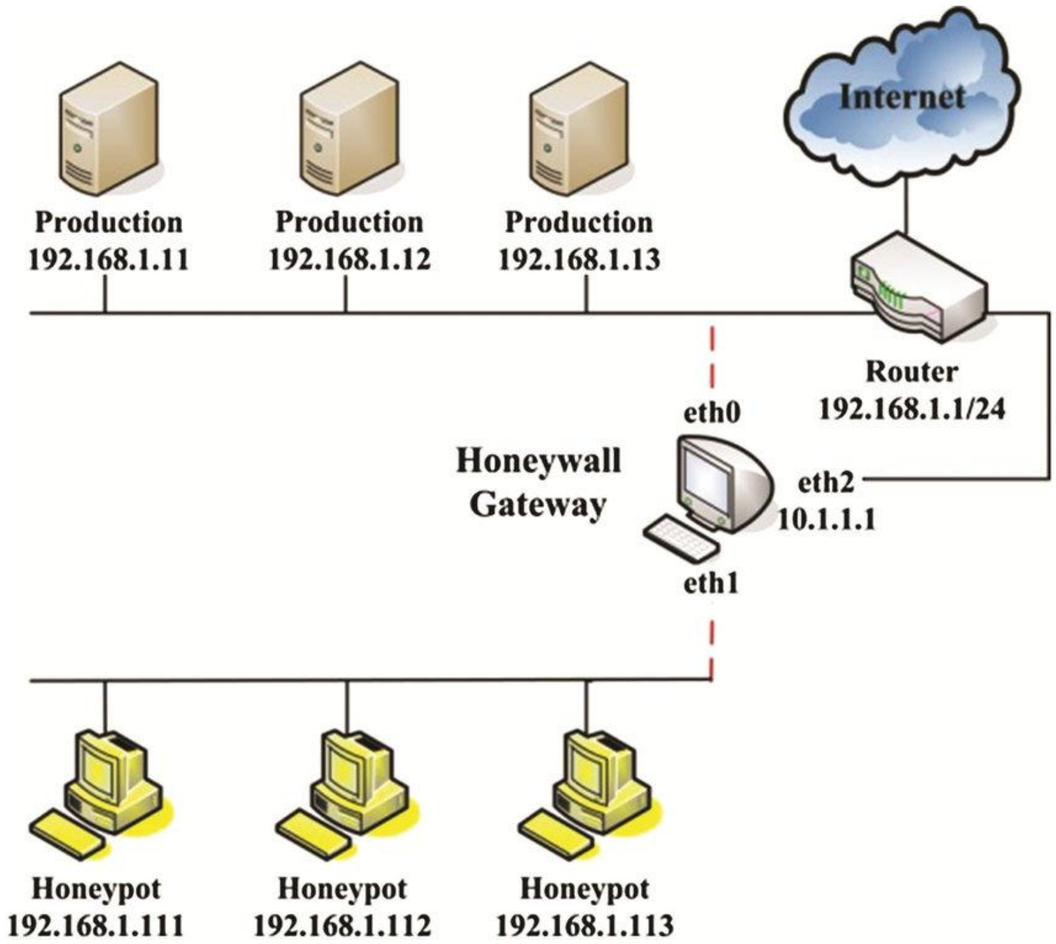
- Se aconseja comprar e instalar los firewalls con las características de IDS e IPS instaladas.



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

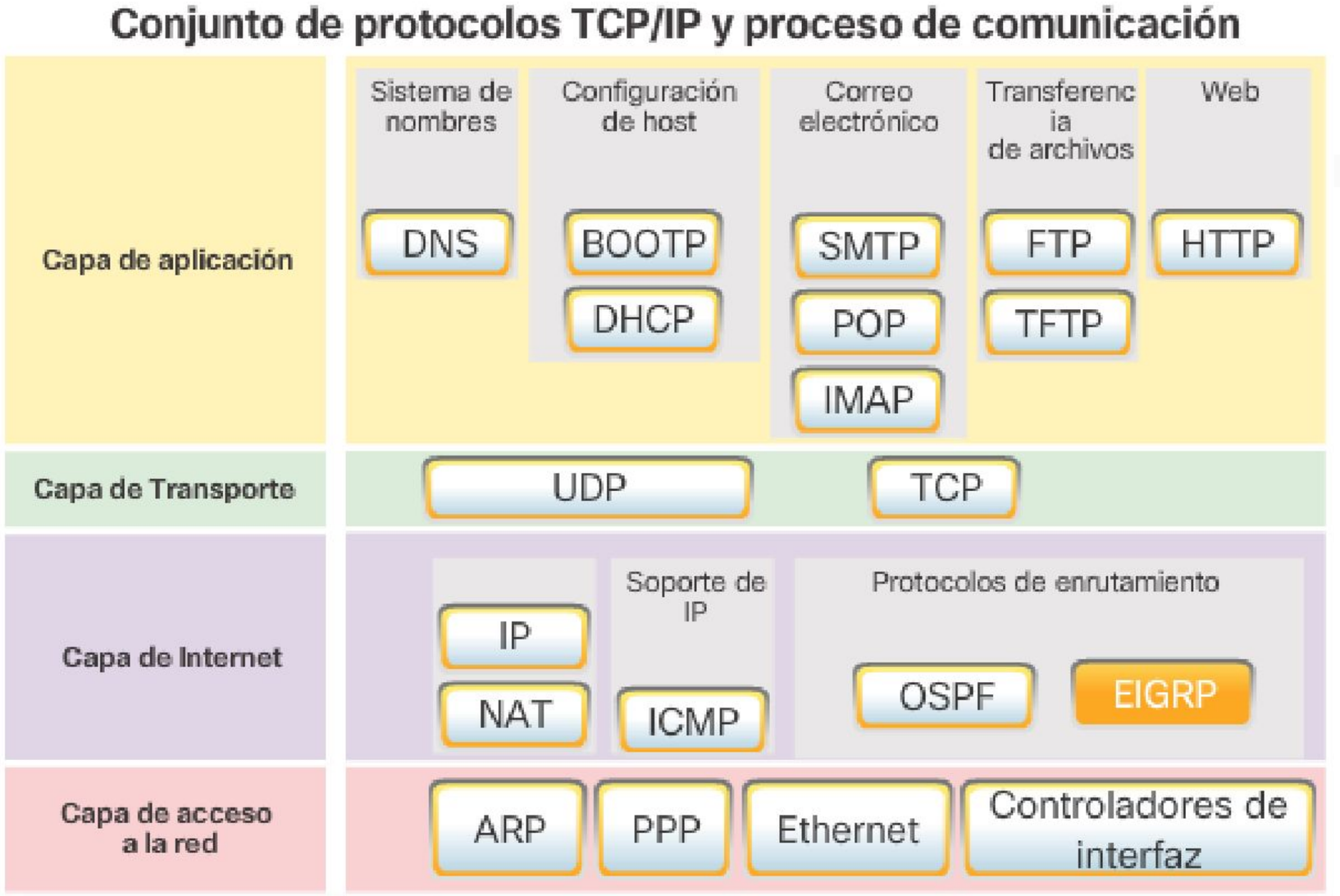
Hardware de Red

- **HoneyPots**
  - Es un sistema informático que se “sacrifica” para atraer ciberataques, como un señuelo.
  - Simula ser un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los cibercriminales y la forma en que operan o para distraerlos de otros objetivos
- **HoneyNets**
  - Es una red de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes.
  - Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.



https://www.researchgate.net/figure/Gen-II-honeynet-architecture_fig3_285598988

Protocolos en el Modelo OSI



https://www.ingenieriasystems.com/2016/10/Creacion-de-Internet-y-desarrollo-de-TCPIP-Suite-de-protocolos-TCPIP-y-proceso-de-comunicacion-CCNA1-V5-CISCO-C3.html

Calcular el Direccionamiento IP de una red

- Para calcular una dirección IP de manera segura y rápida, puedes utilizar una calculadora de subred IP.
- Estas herramientas te ayudan a determinar los valores de la red, utilizando la clase de red, la dirección IP y la máscara de subred.
- A continuación, te presento dos opciones:
- IP CALC
  - https://aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi1
- IPTP Calculadora de subred IP
  - https://www.iptp.net/es_ES/iptp-tools/ip-calculator/
- En internet hay muchas de estas calculadoras.

https://aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi1

WIRESHARK

- **Wireshark** es un analizador de redes líder que permite capturar y analizar paquetes de datos en una red (Sniffer).
- Puedes examinar protocolos, detectar problemas y comprender el tráfico de red.
- Es ampliamente utilizado por administradores de redes, ingenieros y entusiastas de la seguridad,
- Algunas de sus características son:
  - **Captura de paquetes**: Wireshark puede interceptar y mostrar paquetes de datos en tiempo real.
  - **Filtros**: Permite aplicar filtros para analizar solo los paquetes relevantes.
  - **Desglose de protocolos**: Muestra detalles de cada protocolo presente en los paquetes.
  - **Análisis de flujo**: Puede seguir el flujo de datos entre dispositivos.
  - **Estadísticas**: Proporciona estadísticas sobre el tráfico de red.
- Es Potente, gratuito, multiplataforma y con una gran comunidad de usuarios y colaboradores.
- Requiere conocimientos técnicos.

https://www.wireshark.org/


THE
BRIDGE