



Seguridad Activa: Acceso y Control de Redes

Tema 6

Álvaro Rodríguez - IES Alonso de Madrigal (Ávila)
2º SMR

Seguridad Activa: ACCESO a REDES

INTRODUCCIÓN

En las dos unidades anteriores hemos estudiado a fondo cómo proteger nuestra máquina junto con los datos y el software que ejecuta en ella. Pero en una empresa **es raro encontrar una máquina aislada.**

Generalmente están conectadas

- a una **red de área local** (LAN [Local Area Network]) para utilizar los recursos de otras máquinas y para que otras máquinas aprovechen los suyos (por ejemplo, el disco en red NAS)
- A una **WAN** y a **Internet**

Una máquina que ofrece **servicios TCP/IP** debe abrir ciertos **puertos**. A estos puertos pueden solicitar conexión máquinas fiables siguiendo el protocolo estándar, o **máquinas maliciosas.**

SEGURIDAD ACTIVA: ACCESO A REDES

ACTIVIDAD

Objetivo. Vamos a conocer cómo se sabe si un ordenador con Windows está conectado a otra máquina

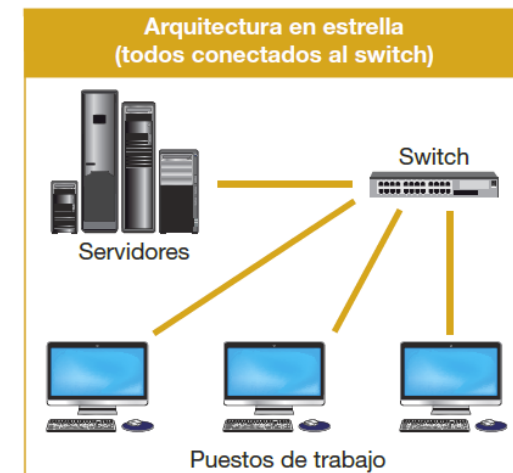
1. En Windows lanzamos la herramienta del monitor de recursos
2. En la ventana del monitor de recursos nos vamos a la pestaña Red
3. Examina los valores que aparecen en el visor de recursos
4. Abre un navegador y entra en una dirección.
5. Comprueba las conexiones existentes
6. Utiliza la herramienta whois en KALI para obtener información sobre alguna IP a la que estás conectado.
7. Utiliza Shodan o Censys para analizar el origen y el dueño de la IP

Seguridad Activa: ACCESO a REDES

SEGURIDAD DE LA ARQUITECTURA

Las primeras redes LAN cableadas eran muy inseguras, porque todos los ordenadores estaban **conectados al mismo cable** (arquitectura en bus, utilizando **hubs**), de manera que cualquiera podía poner su tarjeta de red en modo promiscuo y escuchar todas las conversaciones, no solo aquellas en las que participaba.

Actualmente, utilizamos la **arquitectura en estrella**: cada equipo tiene un cable directo a un puerto de un conmutador de red (**switch**) y por ahí envían sus tramas; el switch envía cada trama de red únicamente hacia su destino.



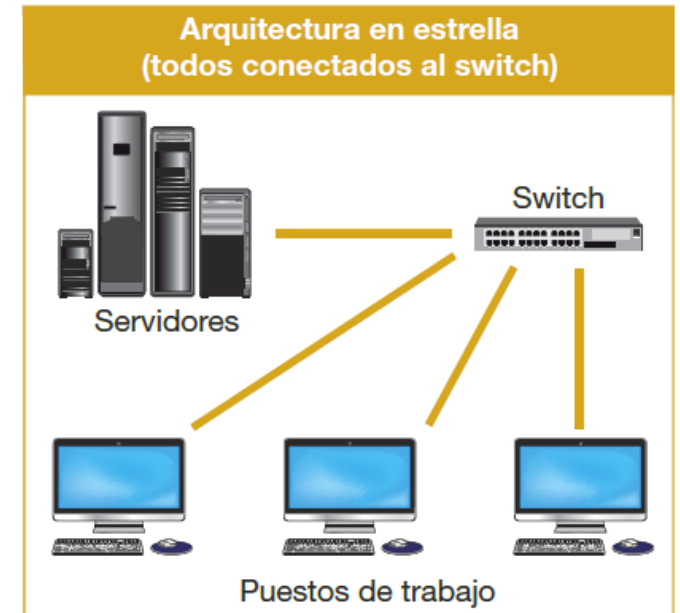
Seguridad Activa: ACCESO a REDES

SEGURIDAD DE LA ARQUITECTURA

Las redes conmutadas tienen sus propias vulnerabilidades:

- Hay que proteger los dispositivos **físicamente**: por ejemplo, un switch, hay que encerrarlo en un armario/rack con llave dentro de una sala con control de acceso. Así evitamos no solo el robo, sino que alguien acceda al botón de reset y lo configure a su modo.
- Hay que protegerlos también **lógicamente**: ese mismo switch, debe tener usuario/contraseña para acceder a su configuración.

Hay que hacer un diseño seguro gracias a la **segmentación**. Por ejemplo, hacer grupos de puertos en un switch, ya que suelen estar conectados grupos de máquinas que nunca necesitan comunicarse entre sí (por ejemplo, el departamento de marketing con el departamento de soporte). Debemos **aislarlas** para evitar problemas de rendimiento y seguridad.



Seguridad Activa: ACCESO a REDES



SERVICIOS EN RED

Además de controlar el acceso a las distintas redes y subredes, es necesario controlar, dentro de una red, qué puertos y servicios están ofreciendo sus equipos.

La herramienta más habitual para el escaneo de puertos y servicios es [Nmap](#). Con Nmap podemos llevar a cabo muchas tareas para controlar nuestra red:

- Listar las máquinas conectadas y activas (encendidas) en la red
- Enumerar puertos abiertos en cada máquina (tanto TCP como UDP)
- Comprobar qué servicio hay detrás de cada puerto e información sobre él (versión, datos que ofrece el servicio...)
- Auditar cada servicio en busca de vulnerabilidades o información relevante (sistema operativo, usuarios, recursos...)

Cuando comprobamos el estado de un puerto podemos encontrarnos que esté:

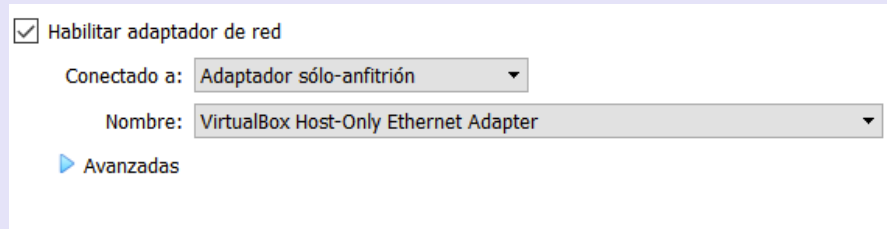
- **Open (Abierto).** Nos indica que una aplicación acepta conexiones TCP o paquetes UDP en este puerto. El encontrar este tipo de puertos es el objetivo principal del sondeo de puertos, tanto para atacantes, que los utilizan para entrar al sistema, como para administradores, que intentan cerrarlos o protegerlos.
- **Closed (Cerrado).** Este tipo de puertos es accesible, respondiendo a las peticiones de Nmap, pero no tiene ninguna aplicación que acepte conexiones o paquetes. Se recibe una respuesta que indica que no se permite la conexión.
- **Filtered (Filtrado).** Nmap no puede determinar si este tipo de puertos se encuentran abiertos o no, ya que no se recibe respuesta ante una petición de conexión.
- **Unfiltered (No filtrado).** Este estado indica que el puerto es accesible, pero que Nmap no puede determinar si se encuentra abierto o cerrado. Solamente el [sondeo ACK](#), utilizado para determinar las reglas de un cortafuegos, clasifica a los puertos según este estado.

SEGURIDAD ACTIVA: ACCESO A REDES

CREACIÓN DEL ENTORNO

Instala una máquina virtual con Metasploitable


Configura tanto la máquina de Metasploitable como la de Kali/Parrot con el adaptador de red en modo "sólo anfitrión"



☒ Habilitar adaptador de red

Conectado a: Adaptador sólo-anfitrión ▼

Nombre: VirtualBox Host-Only Ethernet Adapter ▼

 Avanzadas

Así, se ven entre sí, y ven también al ordenador anfitrión dentro de su red, pero a nadie más. Utiliza el comando ping para comprobar si se ven entre sí las dos máquinas virtuales y para ver si tienen conexión a internet

(El comando [ping](#) Sirve para determinar si una dirección IP específica o host es accesible desde la red o no)

Análisis de los servicios de red

Network Mapper (NMAP) es una herramienta extremadamente avanzada que se puede utilizar para:

- i. Reconocimiento y enumeración: Descubrir hosts activos, segmentos de red, deducir roles...
- ii. Análisis: Detectar la versión de los servicios en puertos TCP y UDP, escaneo de vulnerabilidades.
- iii. Explotación: Prueba y evasión de firewall, ejecución de exploits...

La sintaxis básica de nmap es:

```
nmap target opciones
```

Por ejemplo, el siguiente comando escaneará la IP indicada, utilizando los métodos y sistema por defecto:

```
nmap 192.168.0.33
```

Al no poner más opciones utiliza las siguientes, por defecto: `-sT -p --top-ports 1000`

También puede realizarse análisis de varias IP o de una red entera, cuando indicamos la máscara de la subred:

```
nmap 192.168.0.0/24
```

Importante: el uso de nmap puede generar mucho tráfico de red. Los sistemas de detección de intrusos pueden detectarte y bloquearte. Por eso lo usaremos en entornos controlados en máquinas y redes virtuales. En un entorno real es ilegal utilizarlo sin permiso explícito de la máquina objetivo



Análisis de los servicios de red

Las opciones de nmap permiten especificar mucho más qué queremos hacer. Las opciones más importantes son:

`-sn`

Permite descubrir todos los host activos en un determinado segmento de red. Esta opción evita que se hagan escaneo de puertos de las máquinas.

Muy útil para conocer qué equipos están conectados al mismo segmento de red.

```
nmap 10.0.2.15/24 -sn
```

En sistemas como Kali Linux o Parrot se pueden encontrar otras herramientas que hacen esto mismo, como por ejemplo netdiscover

```
root@kali:~# netdiscover -r 10.0.2.15/24
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:f1:ef:7d	1	60	PCS Systemtechnik GmbH



SEGURIDAD ACTIVA: ACCESO A REDES

ACTIVIDAD

Utiliza `nmap` en Kali con una de sus opciones para "DISCOVER HOST", es decir, descubrir hosts en la red.

`Nmap -help`

Observa los ejemplos que aparecen al final de la ayuda de nmap

¿Qué elementos se encuentran visibles para la máquina de Kali? ¿Está la máquina de Metasploitable?

Análisis de los servicios de red

-n:

no realiza una resolución DNS

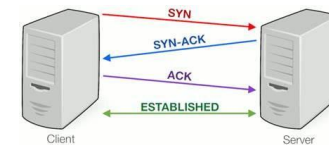
```
nmap 10.0.2.15/16 -sL -n
```

-Pn:

no envía una petición inicial de descubrimiento de host activo, normalmente de tipo ICMP(8), si el host no está dentro de mi mismo segmento de red. Útil contra máquinas activas pero que filtran el tráfico de PING.

-sT:

realiza escaneos a puertos TCP utilizando conexiones TCP completas (Triple Handshake)



-sS:

realiza escaneo a puertos TCP de manera rápida ([SYN port scan](#)).

-sU:

realiza escaneos a puertos UDP.

-sV:

realiza la detección de los servicios de los puertos escaneados.

-sC:

Lanza una serie de scripts de reconocimiento para recabar información sobre los puertos activos



Análisis de los servicios de red

-p

Hace un escaneo solo a los puertos indicados

```
nmap 10.0.2.5 -Pn -n -p 445,3389 -sV
```

Utilizando la opción **-p** hace un escaneo a los 63535 puertos posibles

Podemos indicar varios puertos separando con “,” o un rango de puertos utilizando “:” **-p 21,22,80:1000**

--script <script_name>:

ejecuta el script especificado en “script_name”.

Por ejemplo **--script vuln** ejecuta un script que permite comprobar si las versiones de los servicios obtenidos en el análisis tienen vulnerabilidades conocidas.

-oN archivo.txt:

Guarda el resultado del escaneo en un archivo de texto

--min-rate 5000: Permite un escaneo más rápido, en este caso como mínimo a 5000 paquetes por segundo

-A: realiza un escaneo agresivo, incluyendo escaneos de tipo SYN, detección de SO, traceroute y lanzamiento de scripts



Cheat Sheet de NMAP

Seguridad Activa: ACCESO a REDES

PRÁCTICA

Práctica con Nmap



Seguridad Activa: ACCESO a REDES

ACTIVIDAD

Comandos de supervisión de redes

Para tener un correcto control de las redes será necesario utilizar las distintas herramientas que nos aportan los sistemas operativos para llevar a cabo la supervisión y la administración del sistema desde el punto de vista de sus conexiones de red.

Algunos de los comandos de red más importantes de Windows puedes encontrarlos aquí:

<http://trajano.us.es/~fornes/ARSSP/ComandosRedWindows.pdf>

ipconfig

ping

arp

tracert

route

netstat

nbtstat

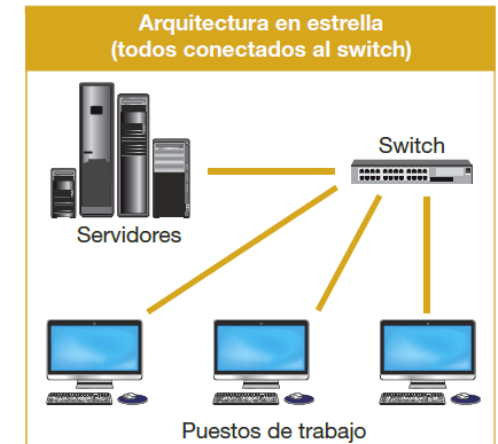
nslookup

Seguridad Activa: ACCESO a REDES

VLAN

Las redes conmutadas tienen sus propias vulnerabilidades:

- Hay que proteger el switch **físicamente**: encerrarlo en un armario/rack con llave dentro de una sala con control de acceso. Así evitamos no solo el robo, sino que alguien acceda al botón de reset y lo configure a su modo.
- Hay que proteger el switch **lógicamente**: poner usuario/contraseña para acceder a su configuración.
- Hay que hacer **grupos de puertos**, porque en un switch suelen estar conectados grupos de máquinas que nunca necesitan comunicarse entre sí (por ejemplo, el departamento de marketing con el departamento de soporte). Debemos **aislarlas** para evitar problemas de rendimiento y seguridad.



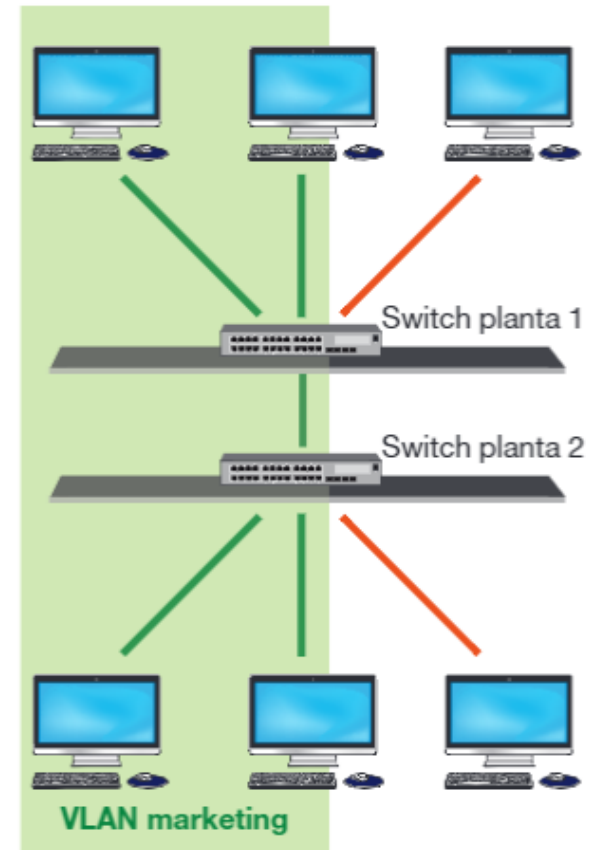
Seguridad Activa: ACCESO a REDES

VLAN

Los grupos de puertos que hacemos en un switch gestionable para aislar un conjunto de máquinas constituyen una VLAN (LAN virtual). Se le llama virtual porque parece que están en una LAN propia, que la red está montada para ellos solos.

Utilizar VLAN mejora el rendimiento y la seguridad, porque **segmenta** la red: esas máquinas solo hablan entre ellas y nadie extraño las escucha.

Una VLAN basada en grupos de puertos no queda limitada a un switch; uno de los puertos puede estar conectado al puerto de otro switch, y, a su vez, ese puerto forma parte de otro grupo de puertos, etc



Seguridad Activa: ACCESO a REDES

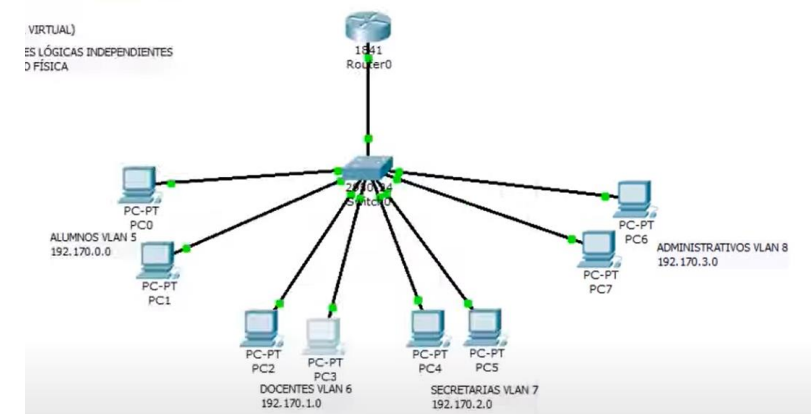
VLAN

Es raro que las VLAN estén completamente aisladas del resto del mundo. Normalmente, necesitarán acceso a Internet, así como conectar con otros servidores internos de la empresa (intranet, disco, backup, correo, etc.).

Para interconectar VLAN (capa 2) generalmente utilizaremos un router (capa 3).

Recordemos:

- Capa 2. En el modelo TCP/IP la capa 2 o capa de enlace tiene una **visión local de la red**: sabe cómo intercambiar paquetes de datos (llamados tramas) con los equipos que están en su misma subred (o VLAN). La comunicación es directa entre origen y destino (aunque cruce uno o varios switch).
- Capa 3. La capa 3 o capa de red tiene una **visión global de la red**: interconecta subredes (o VLAN).



Seguridad Activa: ACCESO a REDES

VLAN CON AUTENTICACIÓN EN EL PUERTO

Hemos protegido el acceso al switch y repartido las máquinas de la empresa en varias VLAN, interconectadas por routers. Pero cualquiera puede meterse en un despacho, desconectar el cable RJ45 del ordenador del empleado, conectarlo a su portátil y ya estaría en esa VLAN.

Como sigue siendo un switch (o un hub), no podrá escuchar el tráfico normal de los demás ordenadores de la VLAN, pero sí lanzar ataques contra ellos.

Para evitarlo, los switch permiten establecer autenticación en el puerto. Se puede gestionar de dos formas:

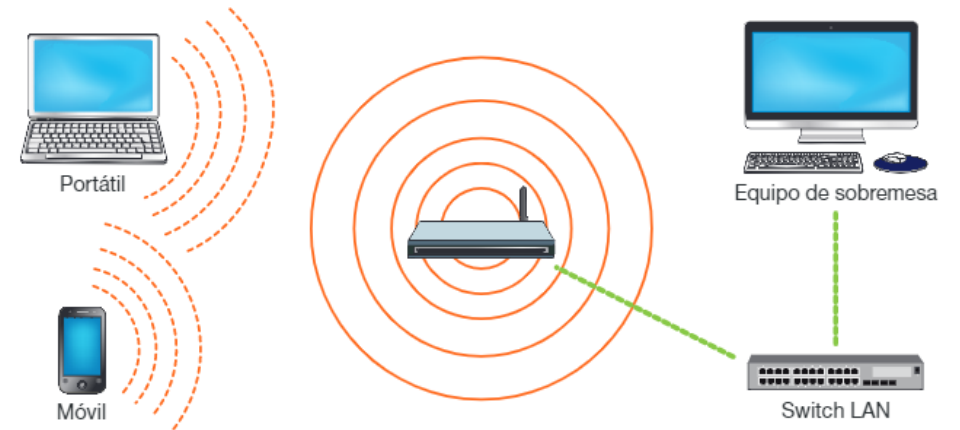
- **Con filtro MAC:** se define qué MAC se puede conectar a cada puerto
- Mediante **RADIUS** en el estándar 802.1X. En esta configuración el switch pedirá usuario y contraseña para dejar conectar a sus puertos. Es más útil dado que las MAC son fácilmente falsificables.

Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS

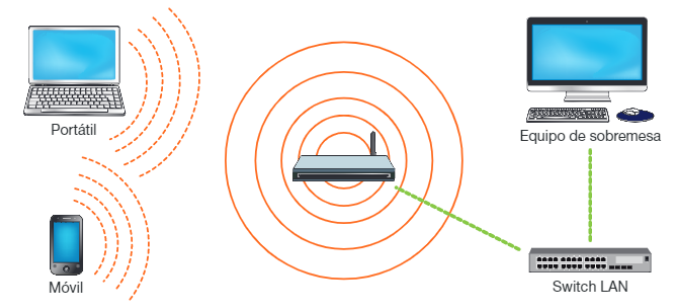
En redes inalámbricas o WLAN (Wireless LAN), el medio de transmisión (el aire) es compartido por todos los equipos y cualquier tarjeta en modo promiscuo puede perfectamente escuchar lo que no debe.

Aunque se pueden hacer redes inalámbricas entre equipos (redes ad hoc), lo más habitual son las redes de tipo infraestructura: un equipo llamado **access point** (AP, punto de acceso) hace de switch, de manera que los demás ordenadores se conectan a él, le envían sus paquetes y él decide cómo hacerlos llegar al destino, que puede ser enviarlo de nuevo al aire o sacarlo por el cable que le lleva al resto de la red (opción más habitual en las empresas, donde la WLAN se considera una extensión de la red cableada)



Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS

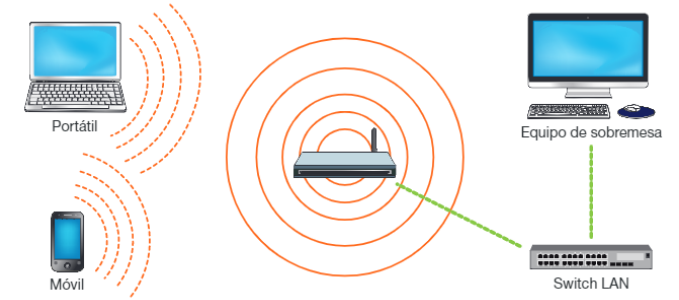


Como ocurría con el switch en las redes cableadas, hemos de:

- Proteger el access point **físicamente**. La protección física es más complicada que en el caso del switch, porque el AP tiene que estar cerca de los usuarios para que puedan captar la señal inalámbrica, mientras que para conectar la toma de red de la mesa con el switch podemos utilizar cable de varias decenas de metros.
- Proteger el access point **lógicamente** (usuario/contraseña).
- Controlar qué clientes pueden conectarse a él (**autenticación**).
- Podemos separar dos **grupos de usuarios**, haciendo que el mismo AP emita varias SSID distintas, con autenticaciones distintas. Estas distintas SSID suelen tener asociada una VLAN etiquetada.
- Sobre todo, hay que **encriptar** la transmisión entre el ordenador y el AP. Así, aunque alguien capture nuestras comunicaciones, no podrá sacar nada en claro

Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS



Mientras que en una red cableada normal (sin autenticación en el puerto), basta con enchufar un cable Ethernet entre la tarjeta de red del equipo y la toma de red en la pared, por ejemplo. En wifi se establecen dos fases: [asociación](#) y [transmisión](#).

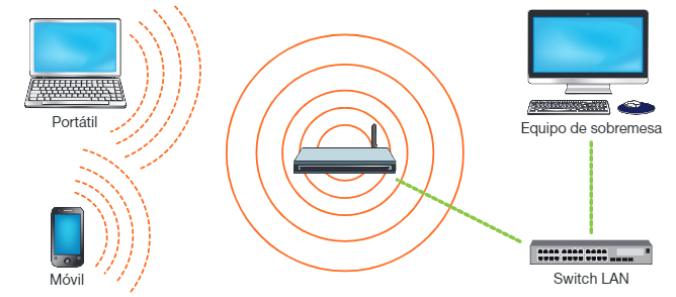
Durante la asociación el usuario elige la SSID a la que se quiere conectar. Entonces la tarjeta inalámbrica contacta con el AP que ofrece esa SSID. Negocian varias características de la comunicación (protocolo b/g/n, velocidad, autenticación...)

La autenticación generalmente se realiza mediante una clave alfanumérica que se registra en la configuración del AP y que el usuario debe introducir para poder trabajar con él. Las AP admiten varios tipos de autenticación:

- [Abierta](#): no hay autenticación, cualquier equipo puede asociarse con el AP.
- [Compartida](#): la misma clave que utilizamos para cifrar la usamos para autenticar.
- [Acceso seguro](#): usamos distintas claves para autenticar y cifrar. El usuario solo necesita saber una, la clave de autenticación: la clave de cifrado se genera automáticamente durante la asociación.
- [Autenticación por MAC](#) el AP mantiene una lista de MAC autorizadas y solo ellas pueden asociarse.

Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS



Existen varios **sistemas de cifrado/autenticación** para redes inalámbricas, siendo los más habituales:

- **WEP**: Ya considerado obsoleto por ser muy vulnerable. Utilizado en cifrado de redes abiertas y en autenticación compartida (la misma clave para autenticar y para cifrar la transmisión)
- **WPA y WPA2**: Pueden usar diferentes sistemas de cifrado como TKIP(Temporal Key Integrity Protocol), PSK (Pre-shared Key o Personal mode) o EAP (Extensible Authentication Protocol). La opción más segura sería WPA2- AES:
 - **WPA2**, el último estándar de encriptación Wi-Fi
 - **AES**, el más reciente protocolo de encriptación

WPA incorpora rotación automática de claves (cada cierto tiempo (varios minutos) el AP y el cliente negocian una nueva clave), y distingue dos ámbitos de aplicación: el personal y el empresarial, con servidor RADIUS para gestionar usuarios y claves.

Una de las grandes vulnerabilidades de WPA/WPA2 no es propiamente el protocolo sino una herramienta que se implementó para facilitar la vinculación entre un cliente y el AP: el sistema WPS

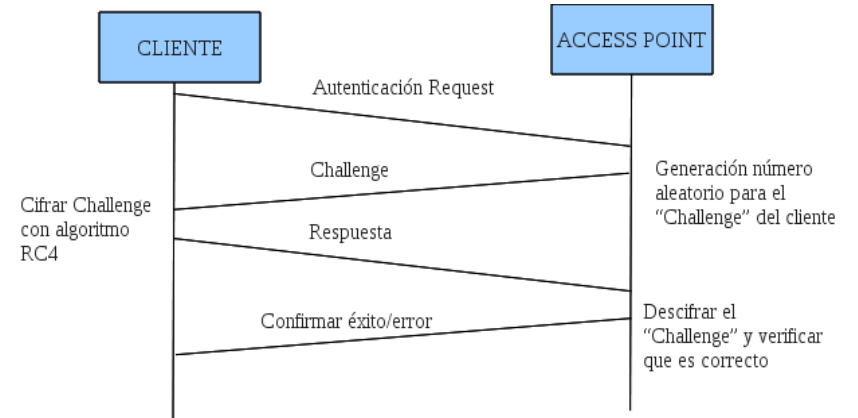
Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS

Vulnerabilidades de cifrado **WEP**:

El protocolo WEP es, de por sí, vulnerable. Se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla (seed en inglés) para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que **no se debe usar la misma semilla para cifrar dos mensajes diferentes**, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un **vector de iniciación (IV) de 24 bits** que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo RC4) para evitar secuencias iguales; de esta manera se crean nuevas semillas cada vez que varía. Para sacar la clave utilizada en la red tan solo debemos capturar muchos paquetes, y luego usar un programa para sacar la contraseña analizando los paquetes capturados.

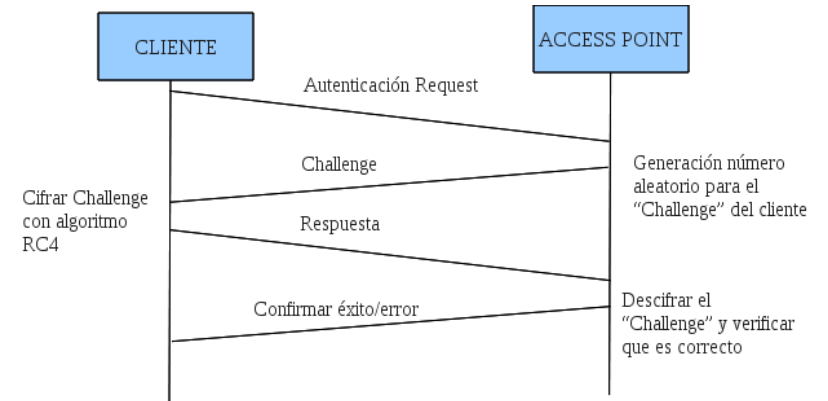


Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS

Un procedimiento típico de ataque a redes bajo cifrado WEP utilizaría:

- **airdump-ng** para capturar todos estos paquetes intercambiados entre cliente y AP
- **aireplay-ng** con el fin de realizar una falsa autenticación con el AP
- otra instancia de **aireplay-ng** con el fin de recolectar peticiones ARP y reinyectarlas de nuevo en la red (bouncing (repetidor) de peticiones ARP), la razón de esto es que el AP generará nuevos IV's ya que reenvía dichos paquetes como broadcast a toda la red, generando rápidamente nuevos IV
- **aircrack-ng** para, una vez pasado un tiempo, intentar crackear la clave WEP, para ello se especifica como parámetro el fichero *.cap generado por airodump-ng



Seguridad Activa: ACCESO a REDES

REDES INALÁMBRICAS

Para **asegurar una red WiFi** y evitar que esta pueda ser hackeada por terceros, hay varios aspectos a considerar, además de la complejidad de la contraseña:

- **PIN WPS (Wireless Protected Setup):** La primera recomendación debe ser inhabilitar WPS si está soportado.
- **Nombre de la red WiFi:** El algoritmo de cifrado de WPA o WPA2 hace uso del nombre de la red WiFi para generar la clave criptográfica. Para evitar el uso de ataques de cracking con [tablas rainbow](#) se debe evitar usar un nombre de red conocido, como WLAN_66 y en su defecto usar nombres nuevos y que no identifiquen a la empresa o al usuario
- **TKIP o AES CCMP:** La recomendación es eliminar el soporte de TKIP si es posible, aunque a día de hoy los ataques no están lo suficientemente extendidos.
- **Contraseñas de administración:** A nivel doméstico es habitual que el punto de acceso WiFi sea un router ADSL o un router de cable. Estos dispositivos pueden estar configurados con contraseñas de administración remotas como admin/admin, 1234/1234, support/support...

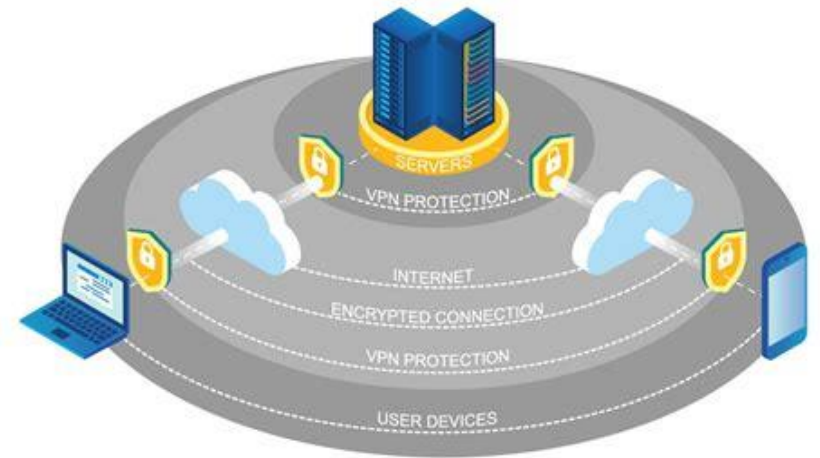
Seguridad Activa: ACCESO a REDES

VPN

Las empresas tienen redes LAN y WLAN para sus oficinas, pero también suelen necesitar que los empleados puedan entrar a esa misma red

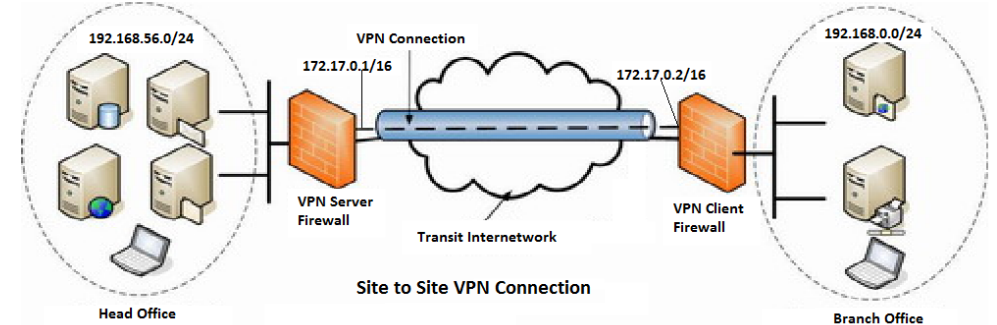
Se busca algo como establecer una VLAN entre el ordenador del empleado y la LAN de la empresa, utilizando Internet como transporte. Estamos hablando de montar una **VPN (Virtual Private Network, red privada virtual)**.

El objetivo final de la VPN es que el empleado (más bien, su ordenador) no note si está en la empresa o fuera de ella. En ambos casos recibe una configuración IP privada (direcciones 10.X.X.X, por ejemplo)



Seguridad Activa: ACCESO a REDES

VPN



El responsable de conseguir esta transparencia es el software de la VPN.

En el ordenador del empleado hay que instalar un [software cliente VPN](#). Este software instala un driver de red, de manera que para el sistema operativo es una tarjeta más. Ese driver se encarga de contactar con una máquina de la empresa, donde ejecuta un [software servidor VPN](#) que gestiona la conexión, para introducir los paquetes en la LAN. La gestión consiste en:

1. Autenticar al cliente VPN.
2. Establecer un túnel a través de Internet. El driver de la VPN en el cliente le ofrece una dirección privada de la LAN de la empresa (la 10.0.1.45, por ejemplo), pero cualquier paquete que intente salir por esa tarjeta es encapsulado dentro de otro paquete. Este segundo paquete viaja por Internet desde la IP pública del empleado hasta la IP pública del servidor VPN en la empresa. Una vez allí, se extrae el paquete y se inyecta en la LAN.
3. Proteger el túnel. Como estamos atravesando Internet, hay que encriptar las comunicaciones (sobre todo si somos una empresa). Los paquetes encapsulados irán cifrados.
4. Liberar el túnel. El cliente o el servidor pueden interrumpir la conexión cuando lo consideren necesario.

Seguridad Activa: CONTROL DE REDES

MECANISMOS DE SUPERVISIÓN DE REDES

A lo largo de este tema vamos a utilizar los siguientes mecanismos de supervisión y control de redes:

- Herramientas Sniffer, que permiten escuchar las comunicaciones existentes en una red
 - Wireshark
 - Tcpdump
- Sistemas de detección de intrusos
 - Snort
- Firewalls
 - Iptables
 - Firewall de Windows
- Proxys

Seguridad Activa: CONTROL DE REDES

WIRESHARK

Es un sniffer de red muy utilizado. Su interfaz básica contiene:

1. El apartado de filtros, que permite obtener sólo paquetes que cumplan determinadas características
2. El apartado de paquetes capturados
3. La especificación de cada capa en el paquete seleccionado (Física, Ethernet, IP, Aplicación)
4. Paquete capturado en bruto (Hexadecimal y ASCII)

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons. The main interface is divided into three panes:

- Packet List (No. 1):** A table showing captured packets. The first packet (No. 4) is selected, showing details like Time (9.028195), Source (10.0.0.100), Destination (239.255.255.250), Protocol (SSDP), and Info (M-SEARCH * HTTP/1.1).
- Packet Details (No. 2):** A tree view showing the layers of the selected packet. The selected packet is an ARP request from 10.0.0.100 to 10.0.0.1. The details pane shows the hardware size (6), protocol size (4), opcode (reply), and MAC addresses.
- Packet Bytes (No. 3):** A pane showing the raw packet data in hexadecimal and ASCII. The data is displayed in a table with columns for offset, hex, and ASCII.

The bottom pane (No. 4) shows the raw packet data in hexadecimal and ASCII format.

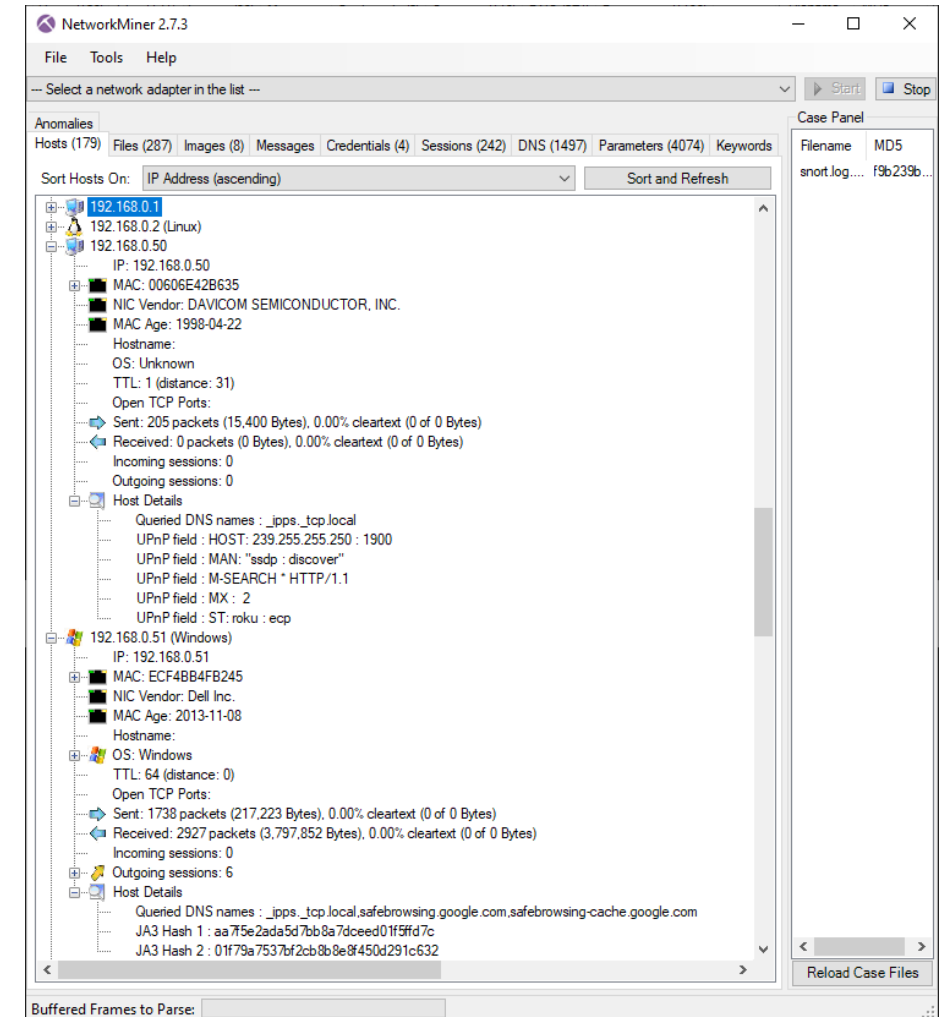
Monitorización de tráfico

ANALIZADORES DE CAPTURAS

Existen herramientas que permiten analizar de una manera más cómoda los paquetes de datos capturados.

Es el caso de [NetworkMiner](#), que permite leer la información contenida en un archivo generado tras una captura de tráfico (generalmente en formato .cap o .pcap)

Es una aplicación para Windows pero puede lanzarse [también en Linux](#)



Seguridad Activa: CONTROL DE REDES

ACTIVIDAD

Captura paquetes con Wireshark mientras tienes las dos máquinas virtuales encendidas (Kali y Metasploitable), y comprueba los resultados al realizar desde Kali a Metasploitable:

- Ping de una máquina a otra
- Descubrimiento de host con Nmap en toda la red
- Escaneo de nmap a la máquina de metasploitable con la opción -sT
- Escaneo de nmap a la máquina de metasploitable con la opción -sU
- Escaneo de nmap a la máquina de metasploitable con la opción -O
- Escaneo de nmap a la máquina de metasploitable con la opción -sV

Seguridad Activa: CONTROL DE REDES

TCPDUMP

La librería de captura de Wireshark (libpcap) es la misma que emplea tcpdump, y la sintaxis de filtrado es muy similar; pero para un mejor conocimiento de la herramienta, consultad las páginas de manual disponibles para tcpdump:

- En Linux `man tcpdump`
- Online http://www.tcpdump.org/tcpdump_man.html

Tcpdump hace la captura de datos y los almacena en un archivo que puede luego ser usado con otro programa como Wireshark o Networkminer

Seguridad Activa: CONTROL DE REDES

TCPDUMP

Una posible llamada a tcpdump sería:

Captura todo el tráfico en un archivo :

```
sudo tcpdump -i en0 -s0 -w ~/capture.pcap
```

- -i en0 captura en la interfaz en0 (el nombre de la interfaz puede obtenerse previamente con ifconfig)
- -s0 utiliza todo el paquete (no truncar – snarf 0)
- -w ~/capture.pcap escribe en el archivo de captura de paquetes ~/capture.pcap

En lugar de -s0 pueden usarse filtros para capturar sólo determinados paquetes.

Algunos ejemplos para esos filtros puedes encontrarlos aquí: <https://juncotic.com/filtros-de-traffic-con-tcpdump/>

Seguridad Activa: CONTROL DE REDES

ACTIVIDAD

Vamos a realizar esta actividad por parejas. Haremos lo siguiente:

- 1.Cada uno de vosotros debe captura paquetes con Tcpdump mientras utilizas internet, puedes entrar en alguna página web, enviar algún correo electrónico...
 - 2.Apunta todas las acciones que vas realizando (no más de 5)
 - 3.Tras obtener el archivo .cap debes intercambiarlo con tu pareja que también te enviará el tuyo.
 - 4.Utiliza NetworkMiner para analizar el archivo cap de tu pareja para averiguar qué acciones realizó
 - 5.Compara las acciones que crees que ha realizado con las que realizó realmente.
- ¿Veis muchas diferencias? ¿Existen conexiones inesperadas? ¿Qué tipo de servidores aparecen y por qué? ¿Qué certificados? ¿Qué tipo de archivos?

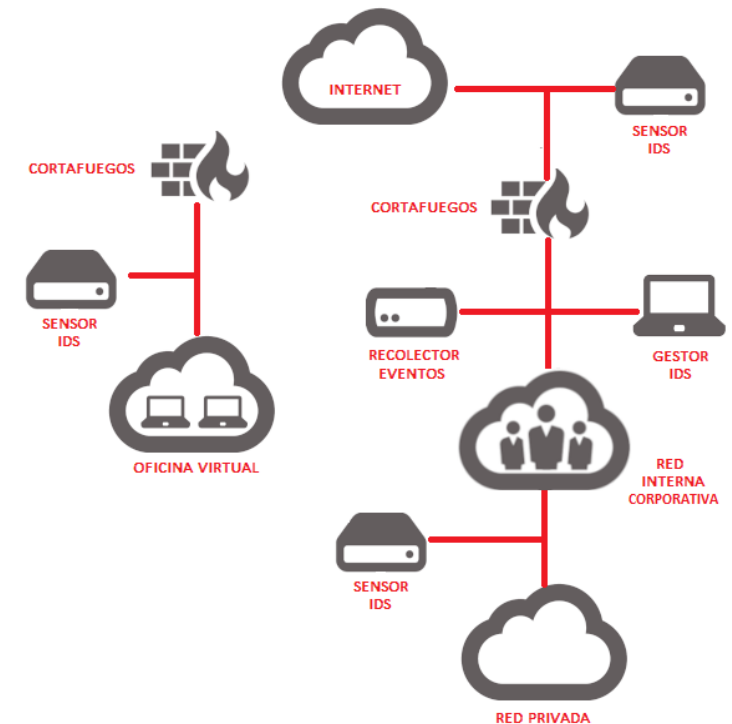
Seguridad Activa: CONTROL DE REDES

IDS, IPS Y SIEM

Son sistemas de protección de las comunicaciones que actúan monitorizando el tráfico que entra o sale de nuestra red.

Vamos a ver tres sistemas diferentes:

- IDS (Intrusion Detection System) o sistema de detección de intrusiones.
- IPS (Intrusion Prevention System) o sistema de prevención de intrusiones
- SIEM (Security Information and Event Management) o sistema de gestión de eventos e información de seguridad

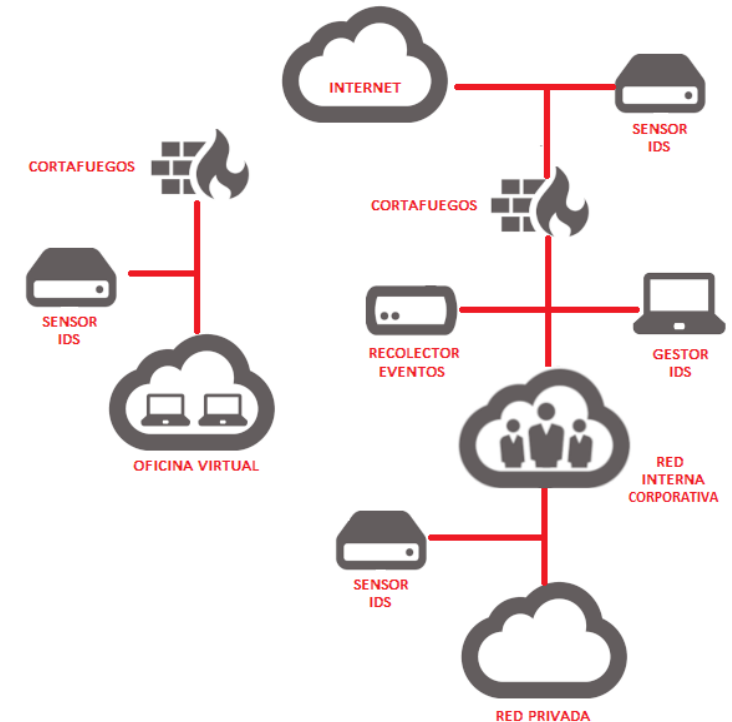


Seguridad Activa: CONTROL DE REDES

IDS (INTRUSION DETECTION SYSTEM) O SISTEMA DE DETECCIÓN DE INTRUSIONES:

Es una aplicación usada para **detectar accesos no autorizados a un ordenador o a una red**, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, **emiten una alerta** a los administradores del sistema quienes han de tomar las medidas oportunas.

Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero **no tratan de mitigar la intrusión**. Su actuación es reactiva

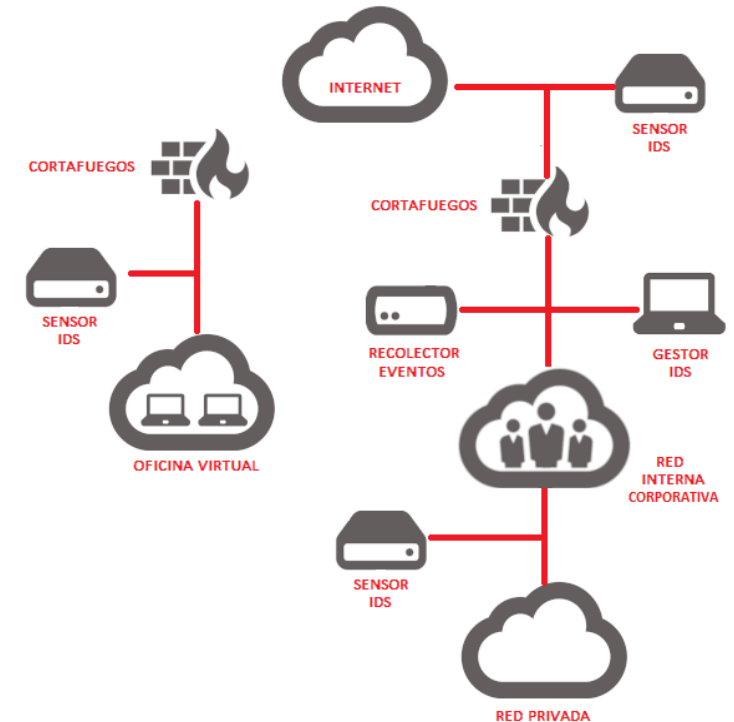


Seguridad Activa: CONTROL DE REDES

IPS (INTRUSION PREVENTION SYSTEM) O SISTEMA DE PREVENCIÓN DE INTRUSIONES

Ayuda a las organizaciones a **identificar** el tráfico malicioso y **bloquea** de manera proactiva el ingreso de dicho tráfico a su red.

En caso de detectarse amenazas, **permiten tomar las medidas adecuadas** según se define en la política de seguridad, como bloquear el acceso, poner en cuarentena a los hosts o bloquear el acceso a sitios web externos que puedan resultar en una posible filtración de seguridad.



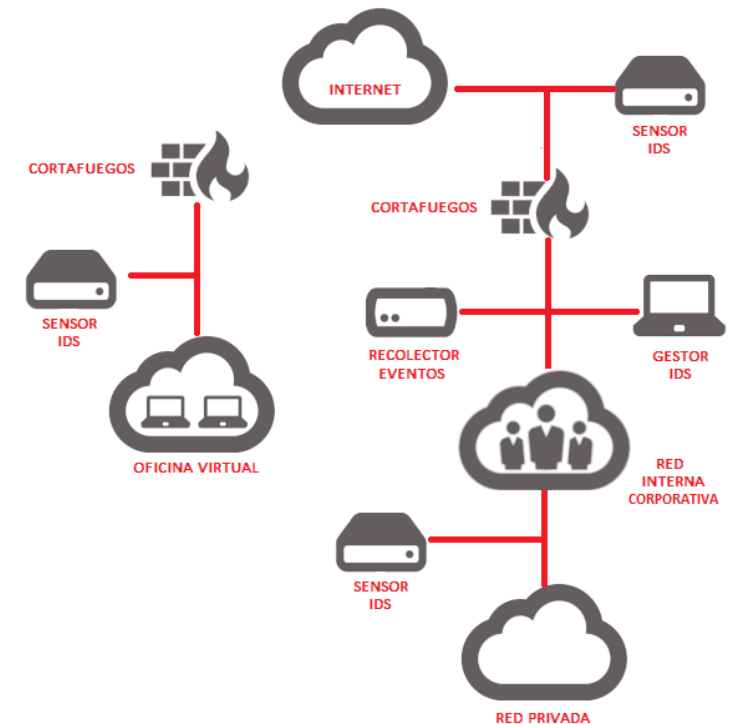
Seguridad Activa: CONTROL DE REDES

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

O SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD

Es un *software* que se utiliza para **proteger a los sistemas de ataques e intrusiones**. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y **permitiendo el control de acceso a la red**, implementando políticas **que se basan en el contenido del tráfico monitorizado**, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con [cortafuegos](#) y [UTM](#) (en inglés *Unified Threat Management* o Gestión Unificada de Amenazas)



Seguridad Activa: CONTROL DE REDES

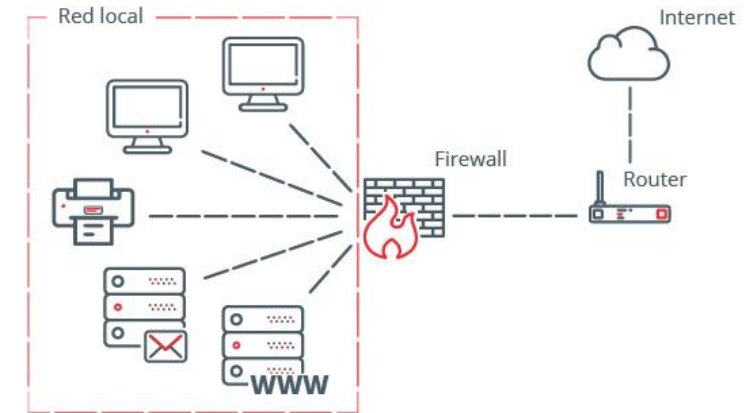
EL FIREWALL

Existen dos elementos fundamentales para minimizar los riesgos derivados de un servidor con acceso desde Internet que pudiera comprometer la seguridad de la organización:

- El cortafuegos o *firewall*
- Un diseño de la infraestructura de red que crea red local “aislada” del resto de la LAN denominada **zona desmilitarizada** o *DMZ*

Los cortafuegos o firewall son unos dispositivos de seguridad cuya función principal es la de **filtrar el tráfico** de red entrante y saliente por medio de una serie de reglas, que permitirán su paso o lo rechazarán. Una vez que una comunicación llega al cortafuegos, esta podrá ser aceptada o rechazada, según se hayan configurado las reglas

Pueden ser **dispositivos específicos dedicados**, o **software**, como el integrado por defecto en el sistema operativo Windows o OS X. (más económicos, pero menos potentes)



Iptables

Es el firewall oficial de sistemas Linux, que forma parte del núcleo del SO desde la versión 2.4

- a. Es ampliamente utilizado hoy en día
- b. Ya no se desarrollan nuevas funcionalidades para él.
- c. Puede trabajar en conjunto con ip6tables, ebtables o arptables.

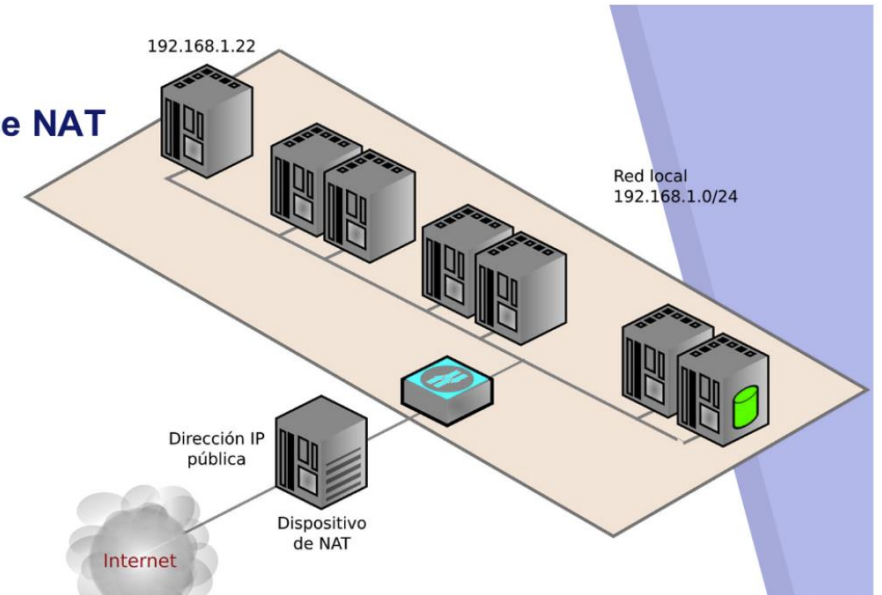
Nftables es el sucesor de [ip, ip6, erpb, arp]tables. Es compatible con iptables, con mayor rendimiento y dando mayor peso al espacio de usuario. Las dos grandes distros Debian y Red Hat, han optado por el uso futuro de Nftables.

Nosotros estudiaremos *iptables*, que permite, además de realizar las funciones de cortafuegos en el filtrado de paquetes hacer NAT o modificar los paquetes que pasan por él.

Recordemos que *NAT (Network Address Translation)* es un sistema que permite:

- Que un equipo con dirección privada pueda conectarse a Internet (SNAT)
- Que un equipo pueda conectarse a un servicio ubicado en una dirección privada (DNAT)

Source NAT



Iptables

En general, cualquier firewall, puede gestionar tres tipos de tráfico:

- Entrante (*INPUT*)
- Saliente (*OUTPUT*)
- Reenviado (*FORWARD*)

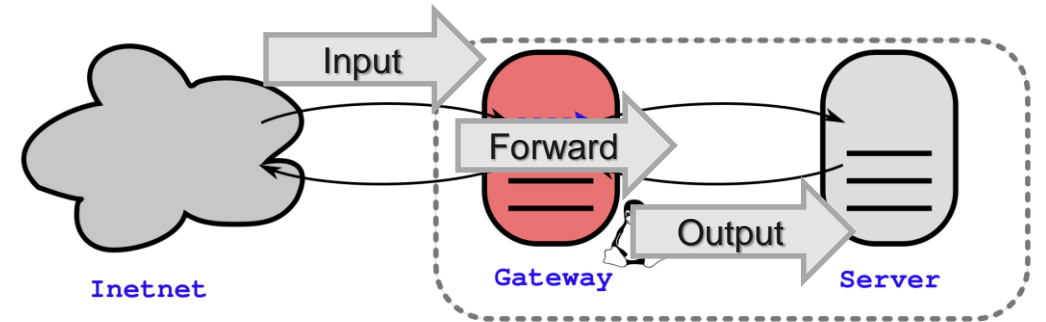
Suele haber dos modos de configuración del firewall, en función de cómo sean las políticas por defecto:

Política por defecto *DROP*

- Más restrictiva: bloquea todo el tráfico y se gestionan las excepciones
- Requiere de un mantenimiento constante
- Es la más recomendable a nivel de seguridad

Política por defecto *ACCEPT*

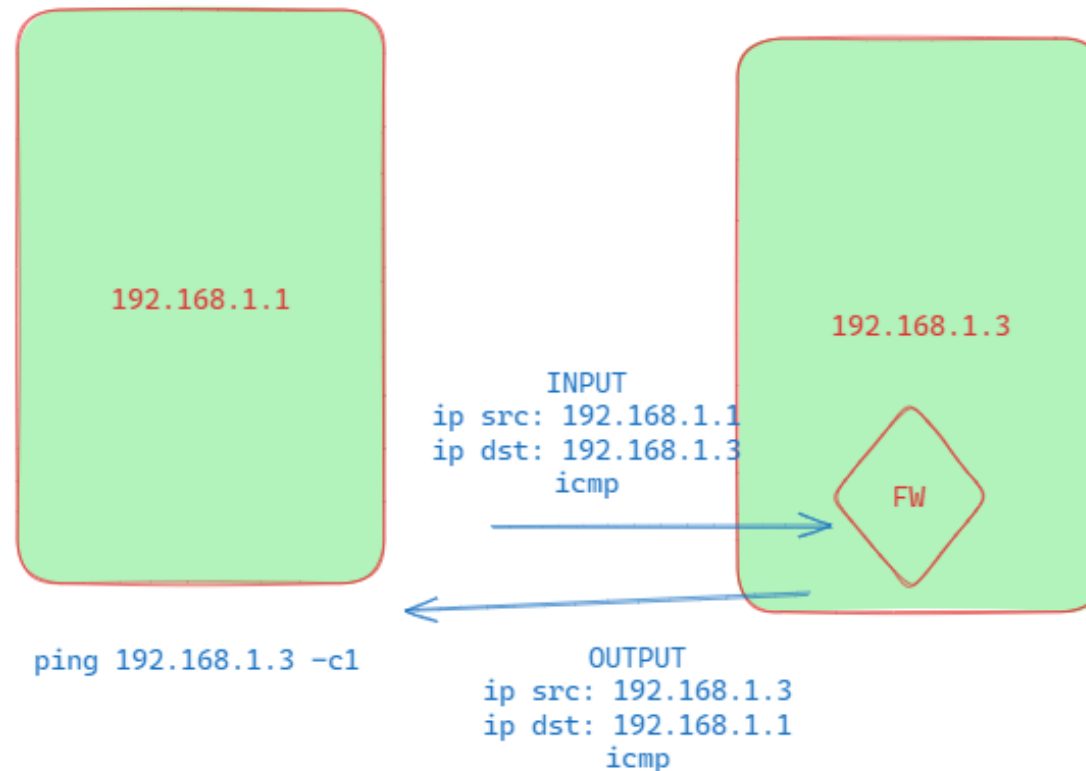
- Menos problemática con respecto a la funcionalidad: se acepta todo, y se gestiona sólo qué queremos bloquear
- Fácil de gestionar
- Es la política por defecto en Iptables



Tipos de tráfico que pasa por el Gateway (donde tendremos el firewall) en una conexión desde internet a un servidor

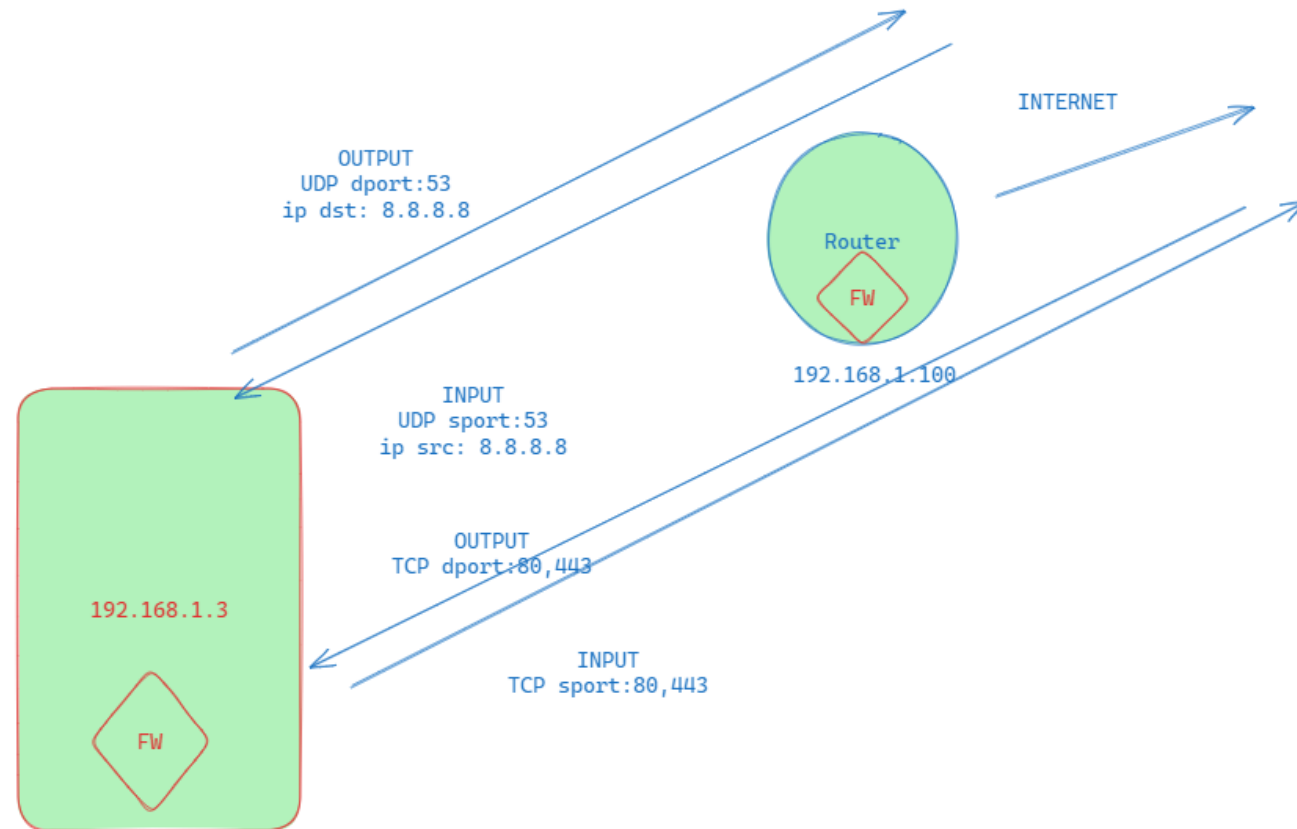
Iptables

Ejemplo de una conexión que se establece al realizar un ping



Iptables

Ejemplo de una conexión que se establece al navegar por la web



Iptables

En Iptables existen diferentes tablas, dentro de las cuáles puede haber *chains* (cadenas). Cada cadena es una lista de reglas con las que se compara cada paquete que pasa por el firewall. En dichas reglas se dice qué debe hacerse si un paquete cumple la regla: acetar el paquete, bloquearlo, registrar su paso en un LOG...

Cuando un paquete es analizado por el firewall comprueba secuencialmente todas las reglas, y en caso de que no se cumpla ninguna se ejecuta **la política por defecto**.

Dentro del firewall se comprueba que tipo de paquete es y en función de ello se comprueba la cadena correspondiente

Existen tres tablas principales, cada una de ellas con sus cadenas:

1. **Tabla Filter:** contiene tres cadenas predefinidas:
 - a. INPUT: para los paquetes que van dirigidos al propio cortafuegos
 - b. OUTPUT: Para paquetes generados localmente y que se envían desde el cortafuegos
 - c. FORWARD: La atraviesan los paquetes enrutados a través de esta máquina
2. **Tabla Nat:** contiene 4 cadenas predefinidas:
 - a. PREROUTING: para paquetes que entran en la máquina cortafuegos, antes de decidir qué hacer con ellos
 - b. INPUT
 - c. OUTPUT
 - d. POSTROUTING: para alterar los paquetes que están a punto de salir de la máquina
3. **Tabla Mangle:** destinada a alterar diferentes parámetros de los paquetes (TTL, TOS...). Cuenta con 5 chains predefinidas: Input, Output, Forward, Prerouting y Postrouting

Iptables

Establecer una política por defecto

```
iptables [-t tabla] -P cadena ACCEPT|DROP
```

Las reglas de iptables funcionan como una ACL, se leen secuencialmente hasta que se encuentra una regla aplicable al paquete

Una vez se defina una regla hay que determinar qué hacer

- ACCEPT: Se permite el paso del paquete
- DROP: Se elimina silenciosamente el paquete
- RETURN: No leer más reglas y pasar a la siguiente cadena

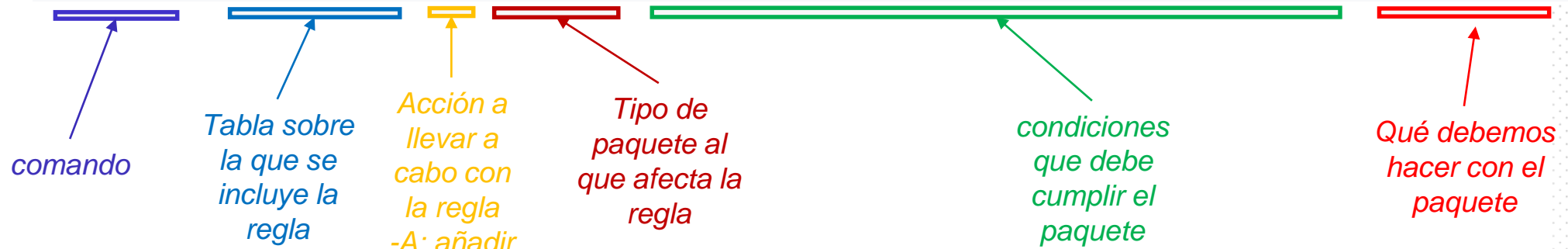
Si no se encuentra ninguna regla se aplica la política de la cadena

Iptables

Las **reglas** de iptables

El comando de inserción de una regla en iptables tiene la siguiente estructura:

```
iptables -t filter -A FORWARD -p tcp -s 192.168.1.2 -d 192.168.2.1 -j ACCEPT
```



Componente	Descripción
-t filter	Vamos a trabajar con la tabla filter (tabla por defecto)...
-A FORWARD	... añadiendo la siguiente regla a su cadena FORWARD.
-p tcp	Selecciona los paquetes cuyo protocolo sea TCP...
-s 192.168.1.2	...cuya dirección origen sea 192.168.1.2...
-d 192.168.2.1	... y cuya dirección destino sea 192.168.2.1.
-j ACCEPT	Acepta esos paquetes para su reenvío.

Iptables

Las reglas de iptables

```
iptables -t filter -A FORWARD -p tcp -s 192.168.1.2 -d 192.168.2.1 -j ACCEPT
```

Los criterios típicos para identificar un paquete son muy diversos:

- -i: adaptador de entrada
- -o: adaptador de salida
- -s: Ip de origen (se puede poner un rango con IP/máscara)
- -d: Ip de destino (ídem)
- -p: protocolo (tcp, udp, icmp...)
 - --sport: puerto de origen
 - --dport: puerto de destino
- otros datos propios de cada aplicación/protocolo

Filtro a nivel físico

Filtro a nivel de red

Filtro a nivel de transporte
/ aplicación

Las acciones a llevar a cabo por los paquetes que cumplan los criterios son:

- **ACCEPT**: Mediante esta acción estamos indicando que el paquete sea aceptado.
- **DROP**: Se elimina el paquete y no se le envía al equipo que hizo la petición ningún mensaje de respuesta.
- **REJECT**: Similar al caso anterior, pero en esta ocasión se manda un paquete ICMP al equipo que hizo la petición para indicarle que no está permitida.
- **DNAT**: modifica la IP de destino. Tiene que llevar asociado el parámetro -to.
- **SNAT**: modifica la IP origen. Al igual que el caso anterior le tiene que acompañar el parámetro -to.
- **MASQUERADE**: Similar a SNAT pero utilizada cuando tenemos una dirección IP dinámica en la interfaz de salida.
- **REDIRECT**: modifica la dirección IP que tenga la interfaz de red de entrada.

Iptables

ACTIVIDAD

- Pon en tu máquina Linux una política por defecto a DROP en todas las cadenas
- Crea reglas con iptables para poder navegar por la web
- Prueba que funciona entrando en cualquier página

Iptables

Creación de reglas:

Append (añade regla al final)	- A	<code>iptables -A [CADENA] [-p PROTOCOLO] [-s IP ORIGEN] [-d IP DESTINO] [-i INTERFAZ ENTRADA] [-o INTERFAZ SALIDA] [-j ACCEPT DROP]</code>
Insert (añade regla al principio)	- I	<code>iptables -I [CADENA] [-p PROTOCOLO] [-s IP ORIGEN] [-d IP DESTINO] [-i INTERFAZ ENTRADA] [-o INTERFAZ SALIDA] [-j ACCEPT DROP]</code>
Check	- C	<code>iptables -C [CADENA] [-p PROTOCOLO] [-s IP ORIGEN] [-d IP DESTINO] [-i INTERFAZ ENTRADA] [-o INTERFAZ SALIDA] [-j ACCEPT DROP]</code>
Delete (borra una regla)	- D	<code>iptables -D [CADENA] [-p PROTOCOLO] [-s IP ORIGEN] [-d IP DESTINO] [-i INTERFAZ ENTRADA] [-o INTERFAZ SALIDA] [-j ACCEPT DROP]</code>
Flush (borra las reglas de una tabla)	- F	<code>iptables [-t tabla] -F [cadena]</code>
Zero	- Z	<code>iptables [-t tabla] -Z [cadena]</code>

Será importante tener en cuenta el orden de creación de las reglas, ya que **cuando una regla puede ser aplicada, se aplica esa y no se revisan el resto.**

Por ello se recomienda añadir **primero las reglas más específicas y después las más generales**

Iptables

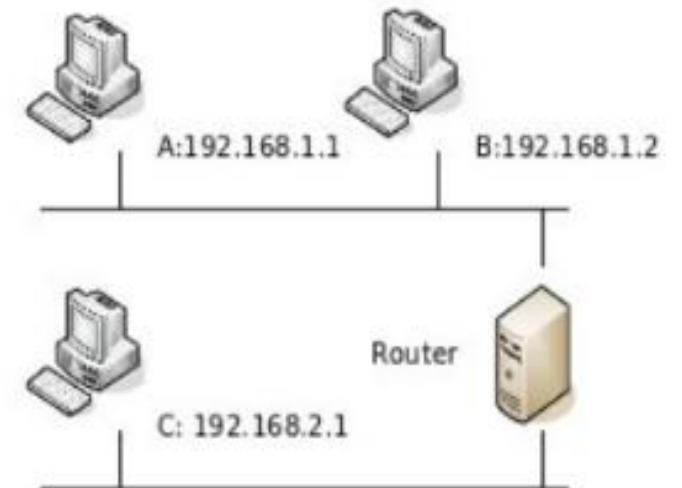
Ejemplo de script de configuración de un firewall:

```
#!/bin/bash
##Script de iptables - Un ejemplo sencillo

##Borramos las reglas de la chain FORWARD de la tabla filter
iptables -F FORWARD

##Establecemos la política por defecto -> DROP
iptables -P FORWARD DROP

##Aceptamos los paquetes TCP entre B y C
iptables -t filter -A FORWARD -p tcp -s 192.168.1.2 -d 192.168.2.1 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -s 192.168.2.1 -d 192.168.1.2 -j ACCEPT
```



Iptables

addrType	Selecciona el tipo de IP --dst-type	<pre>iptables -A INPUT -p udp --sport 68 --dport 67 -m addrtype --dst-type BROADCAST -j ACCEPT</pre>
comment	Añade un comentario --comment	<pre>iptables -A INPUT -p udp --sport 68 --dport 67 -m addrtype --dst-type BROADCAST -m comment --comment "Aceptamos DHCP Discovery" -j ACCEPT</pre>
connlimit	Limita el nº de conexiones paralelas de un mismo cliente --connlimit-above	<pre>iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 3 -j REJECT</pre>
state	Controla el estado de la conexión --state	<pre>iptables -A FORWARD -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT</pre>
iprange	Especifica un rango de IP --src-range	<pre>iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 192.168.1.100-192.168.1.200 -j ACCEPT</pre>
Mac	Inserta reglas por dirección MAC --mac-source	<pre>iptables -A FORWARD -m mac --mac-source 00:23:12:aa:12:45 -j DROP</pre>
Multiport	Especifica varios puertos --dports x:x	<pre>iptables -A OUTPUT -p tcp -m multiport --dports 8000:8800 -j ACCEPT</pre>
Time	Establece horas de inicio y fin --timestart x:x --timestop z:z	<pre>iptables -A FORWARD -p tcp --dport 443 -m time --timestart 13:30 --timestop 14:30 -j ACCEPT</pre>

Iptables

Otras condiciones:

Los protocolos pueden tener sus propias condiciones, por ejemplo:

`-p tcp`

Podemos filtrar en función del estado de la conexión TCP

`-m state --state`

NEW

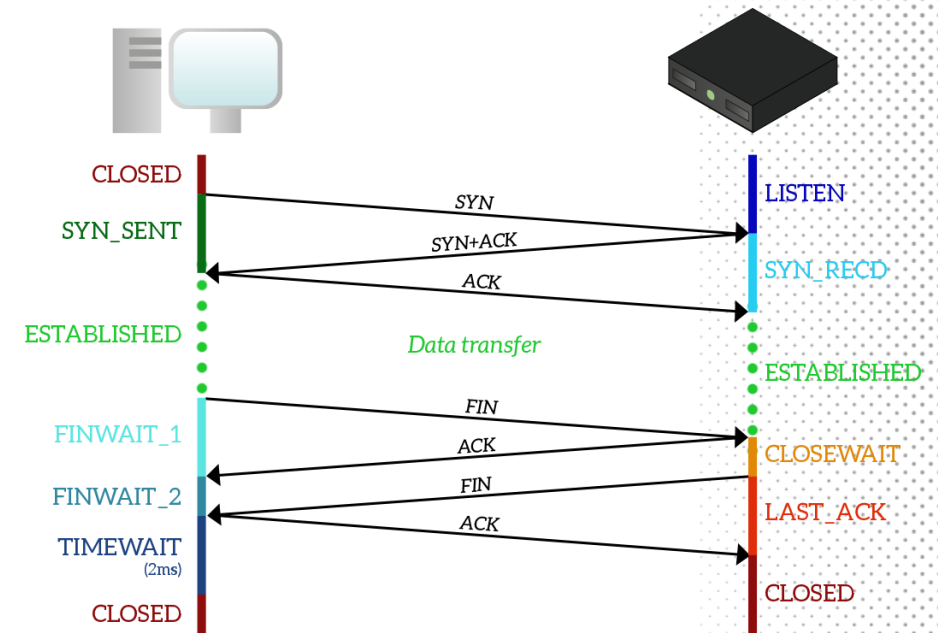
Para conexiones nuevas, aún no establecidas (primer SYN)

ESTABLISHED

Para conexiones ya establecidas (posteriores a SYN)

RELATED

Para conexiones nuevas pero relacionadas con una conexión anterior



```
(kali@kali)-[~/Desktop]
$ #Permitimos a nuestro servidor contestar a conexiones TCP ya establecidas
sudo iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

Iptables

Otras condiciones:

También podemos filtrar un paquete ICMP en función del tipo de paquete.

`-p icmp`

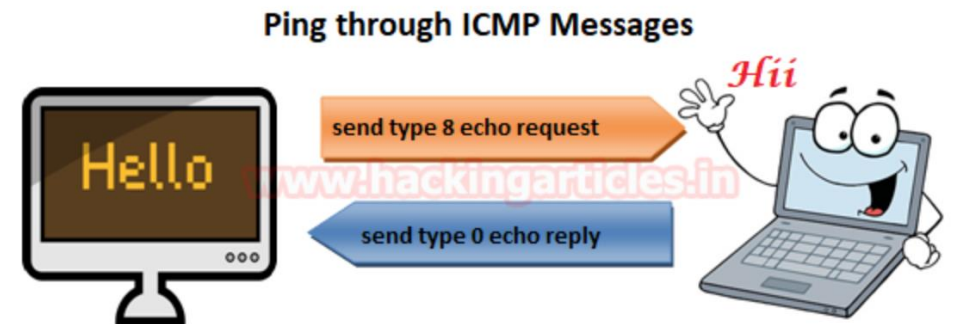
Por ejemplo, al hacer ping tenemos

La petición de PING

`--icmp-type echo-request`

La respuesta

`--icmp-type echo-reply`



```
(kali@kali)-[~/Desktop]
$ ## Denegamos los paquetes de respuesta de PING.
sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP
```

Iptables

Veamos algún ejemplo de regla construida específicamente para crear logs de ciertos sucesos:

Indicamos que se almacenen los accesos a los puertos que vamos a cerrar

```
iptables -A INPUT -p tcp -m tcp --dport 22:23 -j LOG --log-prefix 'INTENTO DE ACCESO A SSH ' --log-level 4
iptables -A INPUT -p tcp -m tcp --dport 20:21 -j LOG --log-prefix 'INTENTO DE ACCESO A FTP ' --log-level 4
iptables -A OUTPUT -p icmp -j LOG --log-level info --log-prefix "IPTABLES: Sale ICMP "
```

Puedes comprobar que, en estos casos, además de la acción LOG, se incluyen:

--log-prefix: Permite incluir en el log un comentario. Esto facilita mucho la búsqueda posterior en el archivo de logs en función de un suceso concreto

--log-level: un número de nivel en función del tipo de suceso.

El LOG generado en iptables se puede consultar utilizando `journalctl -k`, y filtrando el resultado con GREP para que muestre las entradas del log que se necesiten.

Es por ello que conviene añadir en el `--log-prefix` la palabra "IPTABLES", ya que facilitará la búsqueda en el LOG

```
(kali@kali)-[/etc]
$ journalctl -k | grep "ICMP"
Jan 29 18:24:46 kali kernel: IPTABLES: Sale ICMP IN= OUT=eth0 SRC=10.0.2.15 DST=10.0.2.1 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=7298 DF PROTO=ICMP T
YPE=8 CODE=0 ID=41673 SEQ=1
Jan 29 18:24:47 kali kernel: IPTABLES: Sale ICMP IN= OUT=eth0 SRC=10.0.2.15 DST=10.0.2.1 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=7552 DF PROTO=ICMP T
YPE=8 CODE=0 ID=41673 SEQ=2
```


Iptables

Ejemplos de reglas para un firewall:

1.- Reenvío de paquetes desde la interfaz eth1 hacia la interfaz eth0

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

2.- Permitir todo el tráfico entrante desde cualquier dirección (0/0) de la red eth1 hacia cualquier destino (0/0)

```
iptables -A INPUT -i eth1 -s 0/0 -d 0/0 -j ACCEPT
```

3.- Denegar todo el tráfico entrante desde la interfaz eth2 que intente utilizar alguna dirección IP de la red local (192.168.0.0/24)

```
iptables -A INPUT -i eth2 -s 192.168.0.0/24 -j DROP
```

4.- Aceptar todos los paquetes enviados por el protocolo tcp por el puerto 25 en el servidor con ip 217.81.148.217 procedente desde cualquier sitio.

```
iptables -A INPUT -p tcp -dport 25 -s 0/0 -d 217.81.148.217 -j ACCEPT
```

5.- No permitir enviar respuestas a un PING

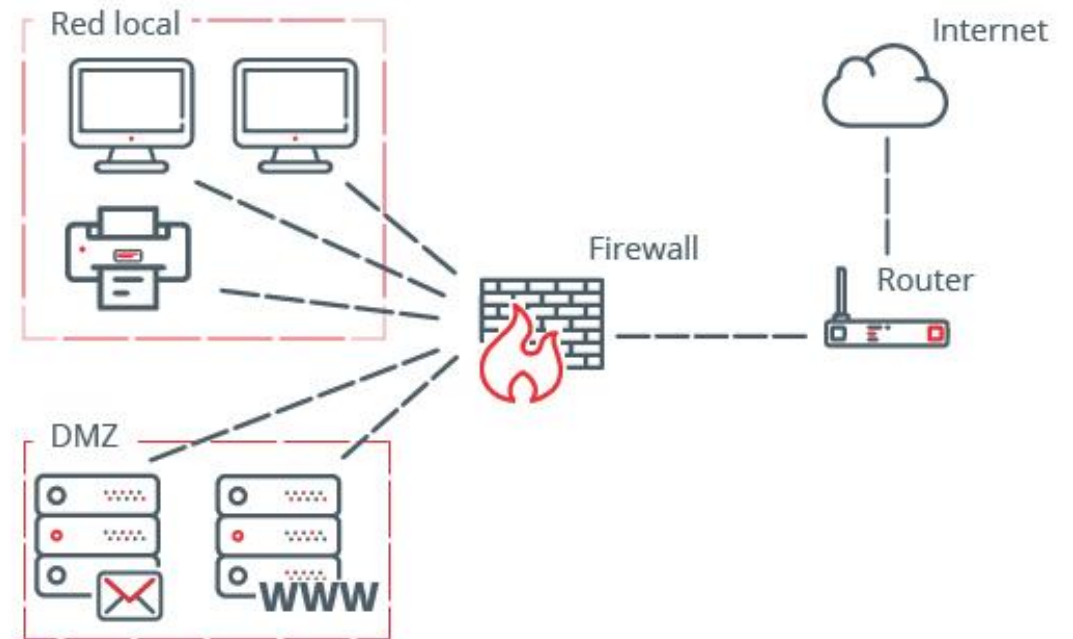
```
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP
```

Seguridad Activa: CONTROL DE REDES

ZONA DESMILITARIZADA DMZ

Una zona desmilitarizada es una **red aislada que se encuentra dentro de la red interna de la organización**. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser **accesibles desde Internet**, como el servidor web o de correo.

La DMZ se configura mediante **Firewalls**.

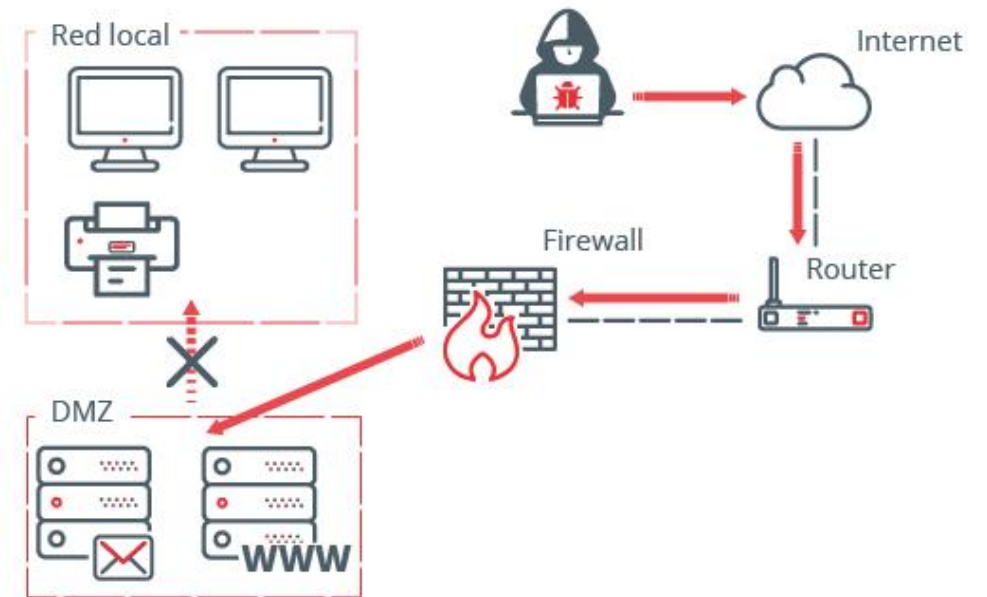


Seguridad Activa: CONTROL DE REDES

ZONA DESMILITARIZADA DMZ

Por lo general, una DMZ permite las conexiones procedentes tanto de Internet, como de la red local de la empresa donde están los equipos de los trabajadores, pero **las conexiones que van desde la DMZ a la red local, no están permitidas**.

Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad. Si un ciberdelincuente comprometiera un servidor de la zona desmilitarizada, tendría muchos más complicado acceder a la red local de la organización, ya que las conexiones procedentes de la DMZ se encuentran bloqueadas.

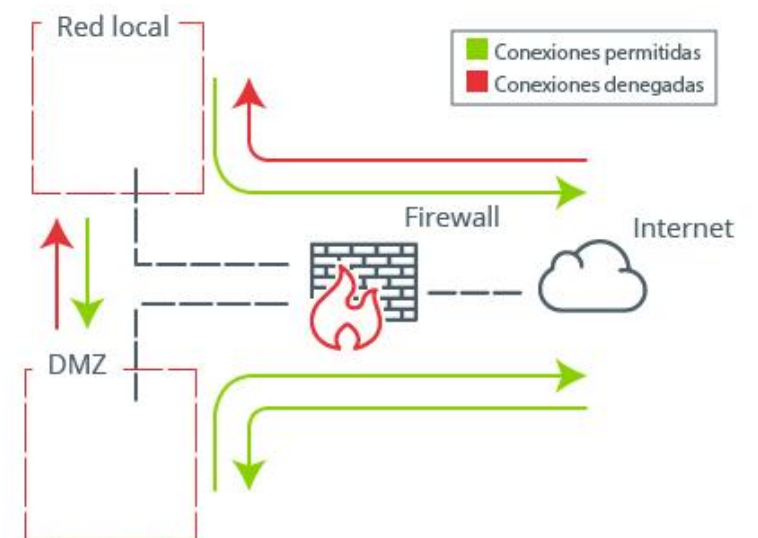


Seguridad Activa: CONTROL DE REDES

ZONA DESMILITARIZADA DMZ

Ejemplo de configuración de un firewall para una DMZ:

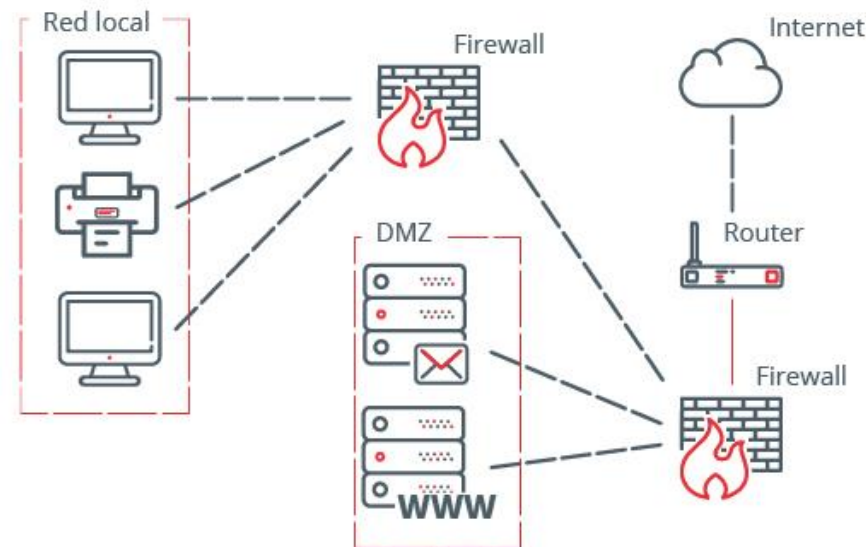
Origen	Destino	Política
Internet	DMZ	Permitido
Internet	LAN	Denegado
DMZ	Internet	Permitido
DMZ	LAN	Denegado
LAN	DMZ	Permitido
LAN	Internet	Permitido



Seguridad Activa: CONTROL DE REDES

DMZ CON DOBLE FIREWALL

No obstante, si se quiere aumentar aún más la seguridad de la red interna frente a un ataque proveniente de la DMZ, se pueden ubicar **dos firewall**.



Seguridad Activa: CONTROL DE REDES

ROUTER COMO DMZ

Muchos **router** que proporcionan los proveedores de Internet, cuentan en su configuración, con una opción para habilitar una DMZ mediante la cual un equipo de la empresa se hace accesible desde Internet. Activar esta opción, **no es muy recomendable**, ya que haríamos que la protección de red dependiera exclusivamente del *router*. Y hay que tener en cuenta que un *router* no es un dispositivo que se haya diseñado específicamente para cumplir las funciones de cortafuegos, siendo sus características de seguridad mucho más reducidas.

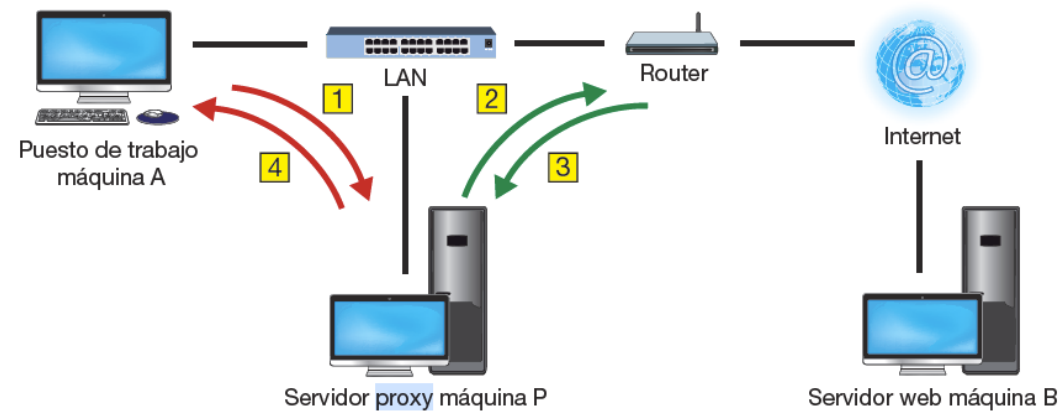
Además, puesto que la DMZ es más propensa a recibir ataques, es recomendable utilizar otro tipo de herramientas de monitorización, detección y prevención. Para ello, se utilizarán de [sistemas de prevención y detección de intrusos](#) o IDS e IPS. Por último, será una tarea crítica mantener los sistemas que se encuentren en la zona desmilitarizada **actualizados a la última versión** disponible.

Seguridad Activa: CONTROL DE REDES

PROXYS

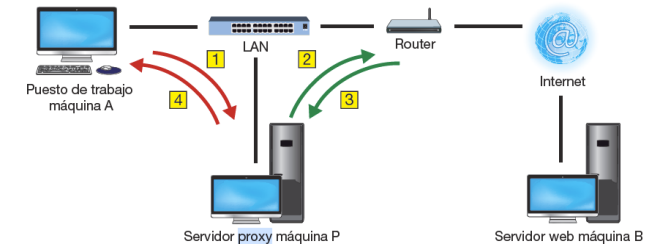
Un **proxy** es un servicio de red que hace de intermediario en un determinado protocolo.

El proxy más habitual es el proxy HTTP: un navegador en una máquina cliente que quiere descargarse una página web de un servidor no lo hace directamente, sino que le pide a un proxy que lo haga por él



Seguridad Activa: CONTROL DE REDES

PROXYS



Los motivos para instalar un proxy pueden ser:

- **Seguridad para el software del cliente** Puede ocurrir que el software del ordenador cliente esté hecho para una versión antigua del protocolo o tenga vulnerabilidades. Pasando por un proxy actualizado evitamos estos problemas, ya que la conexión "desactualizada" se realiza con el proxy, no con el servidor del servicio.
- **Rendimiento.** Si en una LAN varios equipos acceden a la misma página, haciendo que pasen por el proxy podemos conseguir que la conexión al servidor se haga solo la primera vez, y el resto recibe una copia de la página que ha sido almacenada en la **caché** del proxy.
- **Anonimato** En determinados países hay censura a las comunicaciones, por lo que utilizar un proxy del extranjero les permite navegar con libertad.
- **Acceso restringido.** Si en nuestra LAN no está activado el routing a Internet, sino que solo puede salir un equipo, podemos dar navegación al resto instalando un proxy en ese equipo.

Referencias

Seguridad informática. **José Fabián Roa Buendía**. McGraw-Hill España, 2013.

Seguridad informática (Edición 2020) **POSTIGO PALACIOS, ANTONIO**. Ediciones Paraninfo, S.A., May 19, 2020

<https://juncotic.com/filtros-de-trafico-con-tcpdump>

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

[WHITEPAPER \(acens.com\)](https://www.acens.com/whitepaper)