DESCRIPCION CORTAFUEGOS EN AUDITORIAS

- Un firewall es un componente importante en la red de su organización.
- Proporciona a los administradores de red la capacidad de controlar el flujo de tráfico hacia y desde la red.
- El análisis de los firewall logs lo mantiene actualizado sobre todas las transacciones entre la intranet de su organización e internet o cualquier otra red externa.

Logs

- Estos son algunos posibles usos para analizar los firewall mediante logs:
- Listar todas las conexiones negadas por el firewall y resaltar las conexiones sospechosas.
- Estar al tanto de todas las conexiones remotas y VPN a su red.
- Monitorear cualquier cambio en las reglas en las que se basa el firewall.
- Detectar y prevenir cualquier ataque potencial a la seguridad.

Los firewalls son capaces de:

- utilizar el reconocimiento de patrones de firma para analizar y comparar paquetes con una amplia base de datos de amenazas conocidas,
- código malicioso
- vectores de ataque,
- **restringiendo el acceso al tráfico que pueda suponer cualquiera de estos peligros.**

Como evitarlo

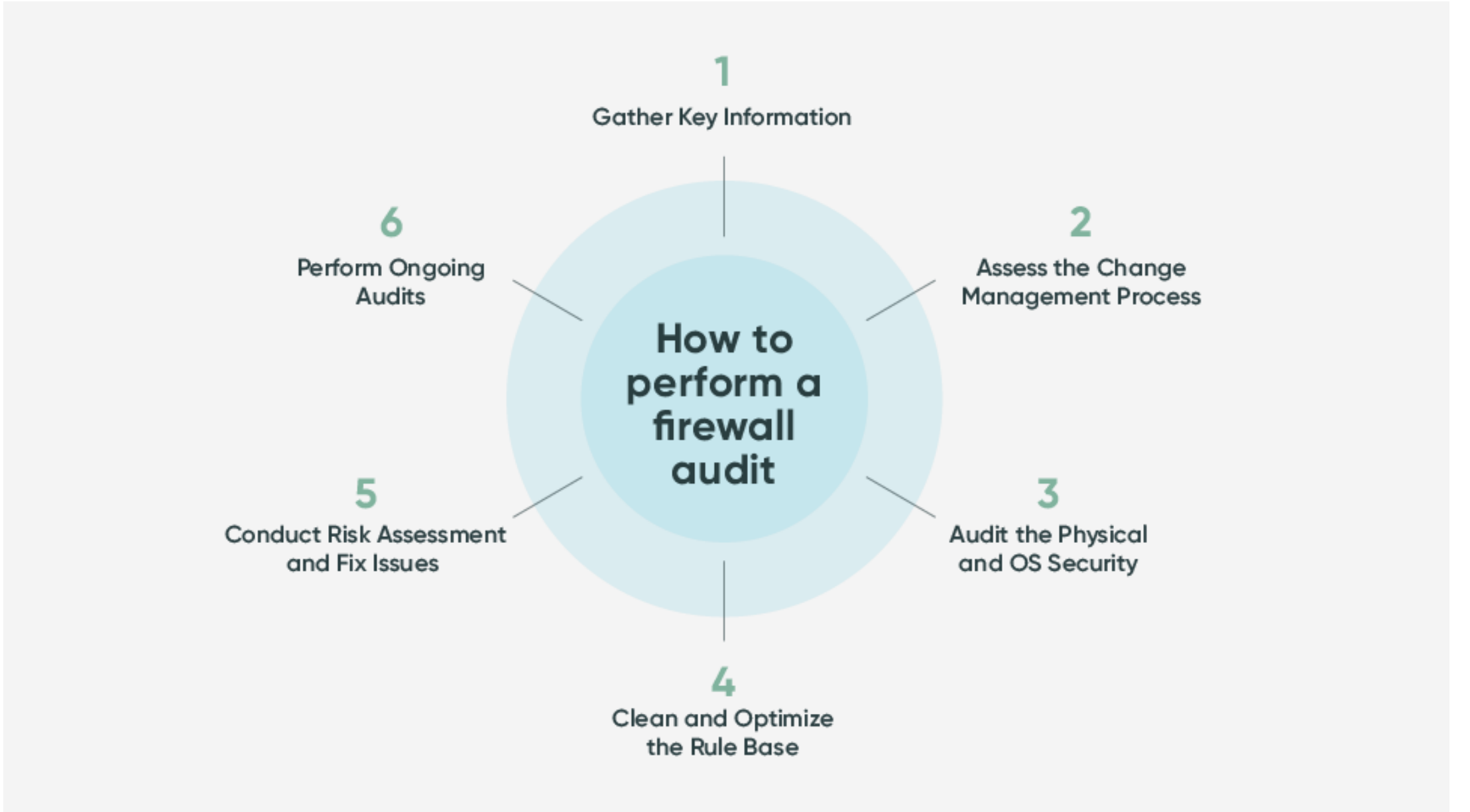
- los firewalls deben actualizarse constantemente para tener en cuenta las amenazas que evolucionan rápidamente y las cargas maliciosas.
- Al mismo tiempo, unas reglas mal configuradas pueden debilitar los firewalls y esa debilidad podría explotarse para obtener acceso no autorizado.
- En ambos casos, la incapacidad del firewall para identificar, aislar y restringir los paquetes maliciosos puede poner toda la red en un peligro significativo.

Control de Accesos

- **El control de accesos de un firewall se consigue mediante:**
- Control de servicios
- Control de direcciones
- Control de usuarios
-
- **Para poder monitorizar la actividad de un cortafuegos se deben de registrar y almacenar la información**

Auditoría de firewall

- El concepto de *auditoría del firewall* se basa en la idea de que la seguridad va más allá de las herramientas; es un proceso continuo en el que las defensas existentes se revisan, auditan y mejoran constantemente para proporcionar la mejor protección posible para los datos y las redes.
- Las auditorías de firewall realizadas de forma regular y coherente son un componente esencial para garantizar la viabilidad del firewall y desempeñan un papel clave en la mejora de la seguridad de la red de toda la empresa.


How to perform a firewall audit
1
Gather Key Information
2
Assess the Change Management Process
3
Audit the Physical and OS Security
4
Clean and Optimize the Rule Base
5
Conduct Risk Assessment and Fix Issues
6
Perform Ongoing Audits

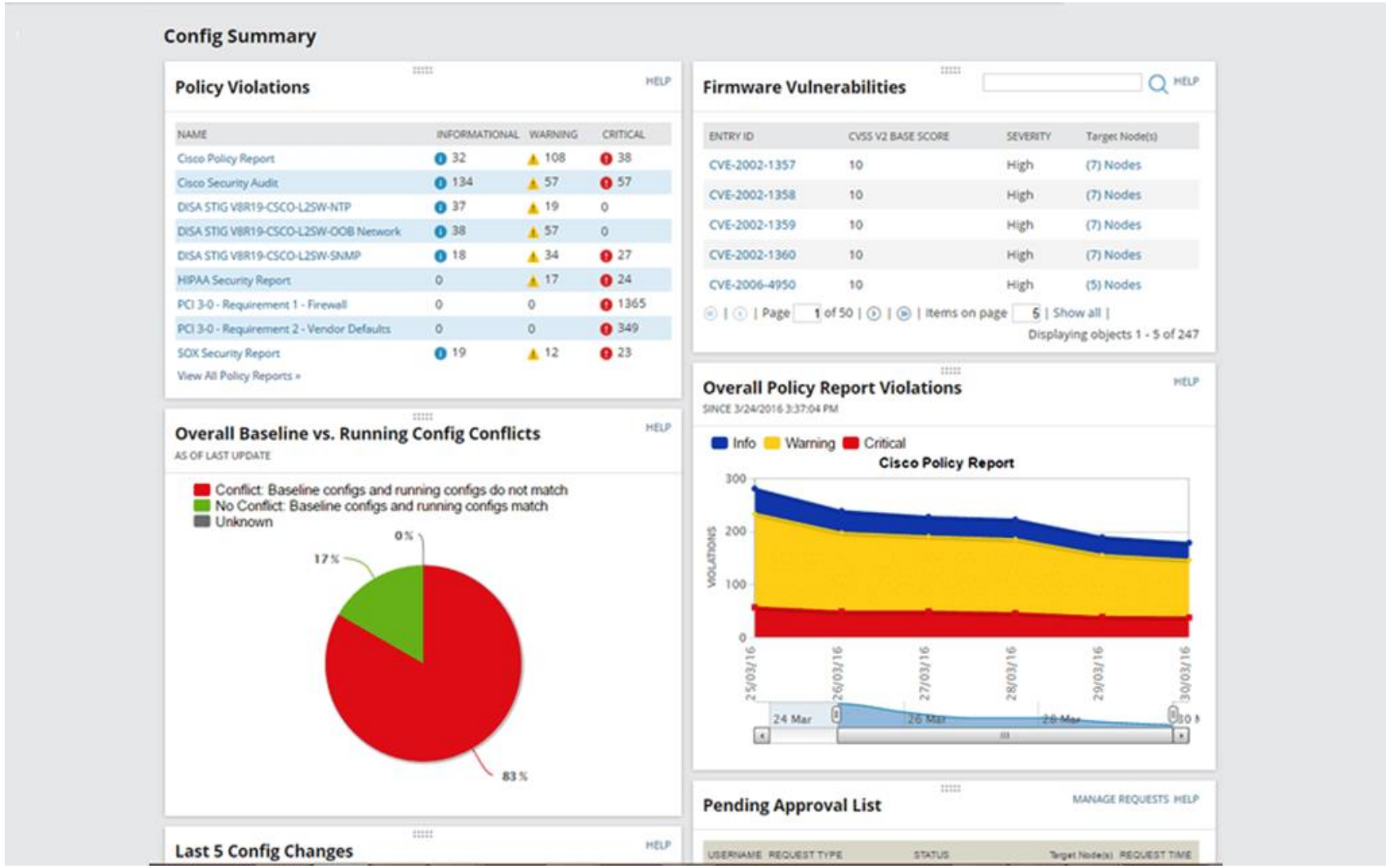
Reglas

- Filtrar origen y/o destino
- Filtrar puertos
- Filtrar tipo de trafico
- Crear listas de control de accesos (ACL)

Protocolos / Puertos

Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	cerrado	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	cerrado	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	cerrado	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UPnP	cerrado	En windows está activado este puerto por defecto.

Reglas de puertos



TIPOS DE FIREWALL

- **Firewall proxy**

- El firewall proxy hace la función de gateway entre dos redes para aplicaciones concretas.
- Los servidores proxy tienen funciones como poder almacenar contenido de caché y seguridad, evitando conexiones directas desde el exterior o no permitiendo que los usuarios puedan conectarse a determinadas webs, o incluso denegarles el permiso.

- **Stateful inspection firewall**

- Es el firewall “tradicional”, un firewall de inspección de estados permite bloquear el tráfico según reglas o criterios en base al estado, puerto y protocolo.

- Monitoriza toda la actividad de red desde que se abre una conexión hasta que se cierra.
- Las decisiones con respecto al filtrado se toman en base a reglas definidas por el administrador.

TIPOS DE FIREWALL

Firewall para gestión unificada de amenazas (UTM)

- Un UTM combina las funciones de un statefull inspection firewall, con IPS (prevención de intrusiones) y las funciones de un antivirus.

- **Firewall de última generación (NGFW)**

- Los firewalls han evolucionado bastante y actualmente son mucho más que un filtrado de paquetes o una inspección de estados. Muchas empresas están implementando firewalls NGFW para detener amenazas como los malwares más avanzados, ransomwares y ataques en la capa de aplicación. Las ventajas que debe incluir un firewall NGFW:

- **NGFW centrado en las amenazas**
- Este tipo de firewall cuenta con las funciones de un firewall de última generación tradicional y también ofrece detección y remediación de amenazas avanzadas. Esto es lo que podrá hacer con un NGFW centrado en las amenazas:
- Conocer qué sectores corren más riesgo, gracias a su completa visibilidad del contexto
- Reaccionar rápidamente a los ataques a través de la automatización de una seguridad inteligente que establece políticas y refuerza sus defensas de manera dinámica
- Detectar de manera más efectiva las actividades evasivas o sospechosas gracias a la vinculación de la red y el evento del terminal
- Reducir de manera significativa el tiempo entre la detección y la limpieza a través de una seguridad retrospectiva que monitoriza de manera continua para buscar actividades y comportamientos sospechosos incluso después de una inspección inicial
- Simplifica la gestión y reduce la complejidad gracias a políticas unificadas que aportan protección durante todo el ciclo del ataque

Funciones de firewall de inspección de estados.

- IPS: prevención de intrusiones.
- Detección de aplicaciones y control que permita visualizar y bloquear aplicaciones que puedan generar una brecha de seguridad y generar riesgos.
- Añadir nuevas fuentes de información.
- Técnicas que permitan detectar y aprender frente a los cambios que surgen diariamente en las amenazas para la seguridad.

Cómo configurar el firewall en 6 pasos

Paso 1: proteja el firewall:

- El acceso administrativo al firewall solo debe concederse a las personas de confianza. Para evitar el acceso de posibles atacantes, asegúrese de que el firewall esté protegido con al menos una de las siguientes acciones de configuración:
- Actualice su firewall con el último firmware recomendado por el proveedor.
- Elimine, deshabilite o cambie el nombre de las cuentas de usuario predeterminadas y cambie todas las contraseñas predeterminadas. Asegúrese de usar solo contraseñas complejas y seguras.
- Si varias personas administrarán el firewall, cree cuentas adicionales con privilegios limitados basados en las responsabilidades. Nunca use cuentas de usuario compartidas. Haga un seguimiento de quién hizo cada cambio y por qué. Un buen registro promueve la diligencia debida al hacer cambios.
- Limite los puntos desde los cuales las personas puedan hacer cambios para reducir la superficie de ataque, es decir, que los cambios solo pueden hacerse desde subredes de confianza dentro de la corporación.

Paso 2: diseñe zonas de firewall y direcciones IP

- Todos los servidores que proporcionan servicios basados en la web (por ejemplo, correo electrónico, VPN) deben organizarse en una zona dedicada que limite el tráfico entrante de Internet, lo que suele conocerse como zona desmilitarizada o DMZ.
- Como alternativa, los servidores a los que no se accede directamente desde Internet deben colocarse en zonas de servidores internas. Estas zonas suelen incluir servidores de bases de datos, estaciones de trabajo y todos los dispositivos de punto de venta (POS) o de voz por protocolo de Internet (VoIP).

Paso 3: configure las listas de control de acceso

- Una vez que se establecen zonas de red y se asignan a las interfaces, empezará a crear reglas de firewall llamadas listas de control de acceso (ACL).
- Las ACL determinan el tráfico que necesita permisos para circular entre las zonas. Las ACL son los componentes básicos que determinan quiénes pueden hablar con qué y bloquean el resto.

Paso 4: configure los demás servicios y registros de firewall

- Si lo desea, active el firewall para que actúe como servidor de protocolo de configuración dinámica de hosts (DHCP), servidor de protocolo de tiempo de red (NTP), sistema de prevención de intrusiones (IPS), etc.

- Desactive los servicios que no piensa usar

Paso 5: pruebe la configuración del firewall

- En primer lugar, verifique que el firewall bloquee el tráfico que debería bloquear según las configuraciones de ACL.
- Esto debe incluir el escaneo de vulnerabilidades y las pruebas de penetración.
- Asegúrese de guardar una copia de respaldo segura de la configuración del firewall para usar en caso de falla.
- Si todas las pruebas salen bien, el firewall estará listo para la producción.
- PRUEBE el proceso de reversión a una configuración anterior.
- Antes de hacer algún cambio, documente y pruebe el procedimiento de recuperación.

Paso 6: administración de firewall

- Una vez que el firewall esté configurado y en funcionamiento, deberá hacerle mantenimiento para que su funcionamiento sea óptimo.
- Asegúrese de actualizar el firmware, monitorear los registros, realizar análisis de vulnerabilidad y revisar las reglas de configuración cada seis meses.

ACL

- Las listas de control de acceso son uno de los conceptos más usados en seguridad de redes y tienen como objetivo el filtrado de tráfico. Una ACL está formada por un conjunto de sentencias que permitirán o denegarán un tráfico determinado.

- Para tomar dicha decisión, el paquete se irá comparando con cada sentencia hasta que coincida con una de ellas, siendo en ese momento donde se ejecutará la opción configurada (permit / deny). Es por ello que el orden en que estén expuestas las reglas es crucial para obtener el funcionamiento deseado.

ACL: Tipos de Access-list

- Según el propósito buscado, podremos configurar el tipo de ACL que más se adecúe a nuestro escenario. Podemos elegir entre estos cuatro grupos:
- Standard Se puede concretar la dirección IP (*) de origen o del destino (o de ambos)
- Extended Se puede añadir el tipo y el número de puerto
- Extended MAC El filtrado se realiza en base a las direcciones MAC especificadas
- Extended Expert Combina e incluye todas las anteriores opciones

NAT

- Cada uno de los dispositivos que hay conectados en nuestra red tienen una **dirección IP única**.

- Aquí podemos mencionar ordenadores, móviles o cualquier otro equipo. Esto es necesario para que esté conectado a Internet y el router lo detecte y pueda funcionar con normalidad. El traductor de direcciones de red lo que hace (ya sea en el router, módem o dispositivo que sea) es proporcionar una dirección IP pública a toda esa red, a todo el conjunto de equipos.