SEGURIDAD PERIMETRAL

Ing. Nelson Belloso

CLASE 15

Diseño de redes
de datos DRD101

AGENDA

Malware

Seguridad Perimetral

Firewall

Zona DMZ

MALWARE

Software - Malicioso diseñado para alojarse en un dispositivo sin su consentimiento. Todo virus es un malware y puede adquirirse desde un clic en una pagina maliciosa, clic en un archivo vinculado en un correo, descarga de software gratuitos.

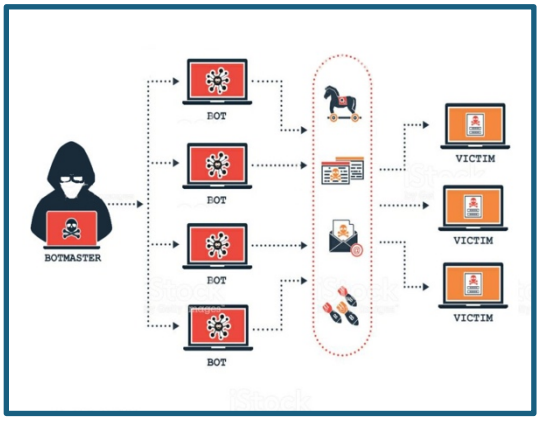
- **Rasomware:** Es la versión malware de la nota de rescate de un secuestrador. Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker.

- **Spyware:** Recaba información sobre un dispositivo o red para luego enviársela al atacante. Los hackers suelen utilizar spyware para supervisar la actividad en Internet de una persona y recopilar datos personales, incluidas credenciales de inicio de sesión, números de tarjeta de crédito o información financiera.

- **Gusanos:** Un gusano infecta un equipo y después se replica y se extiende a dispositivos adicionales
  Permanece activo en todas las máquinas afectadas.
  Son mensajeros para instalar malware adicional.
  Causan daño a las máquinas anfitrionas
  Dañan las redes con demandas de ancho de banda.

- **Adware:** someten a la víctima a publicidad no deseada. Algunos son juegos gratuitos y las barras de herramientas para el navegador. Recaban datos personales para personalizar anuncios. Aunque la mayoría del adware se instala de forma legal, no por ello es menos molesto que otros tipos de malware.

- **Botnet:** Una red de equipos informáticos ejecutando un malware. Los atacantes infectan un grupo de equipos con software malicioso conocido como (**boots**), capaz de recibir órdenes desde su controlador. para coordinar ataques, enviar spam, robar datos y crear anuncios falsos en su navegador.

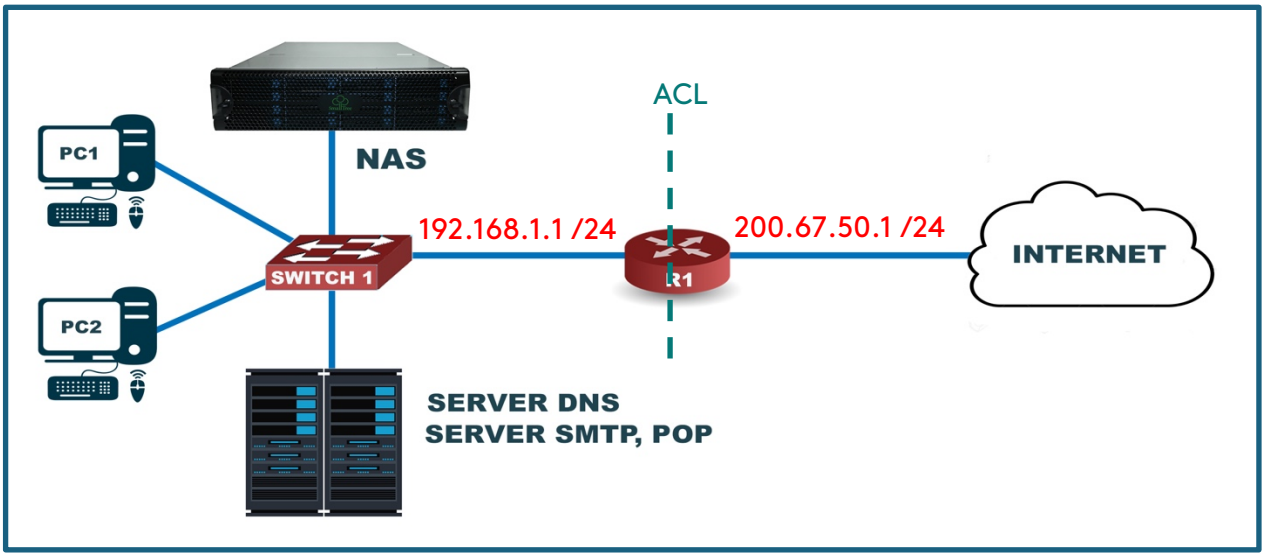


- **Ingeniería social:** Los ataques mas comunes incluyen correos electrónicos de phishing, vishing (llamadas telefónicas de personas que se hacen pasar por una organización respetada) y baiting. Generando paginas clonadas en las cuales solicitan las credenciales.

- **Spam:** son mensajes no solicitados, sobre todo de tipo publicitario, y que son enviados de forma masiva.

SEGURIDAD PERIMETRAL

Edad Media Ciudades amuralladas la defensa contra los ataques externos, comienzan en el perímetro de nuestras instalaciones. Donde lo mas sencillo y lo mas seguro es que todos los accesos sean por una única puerta

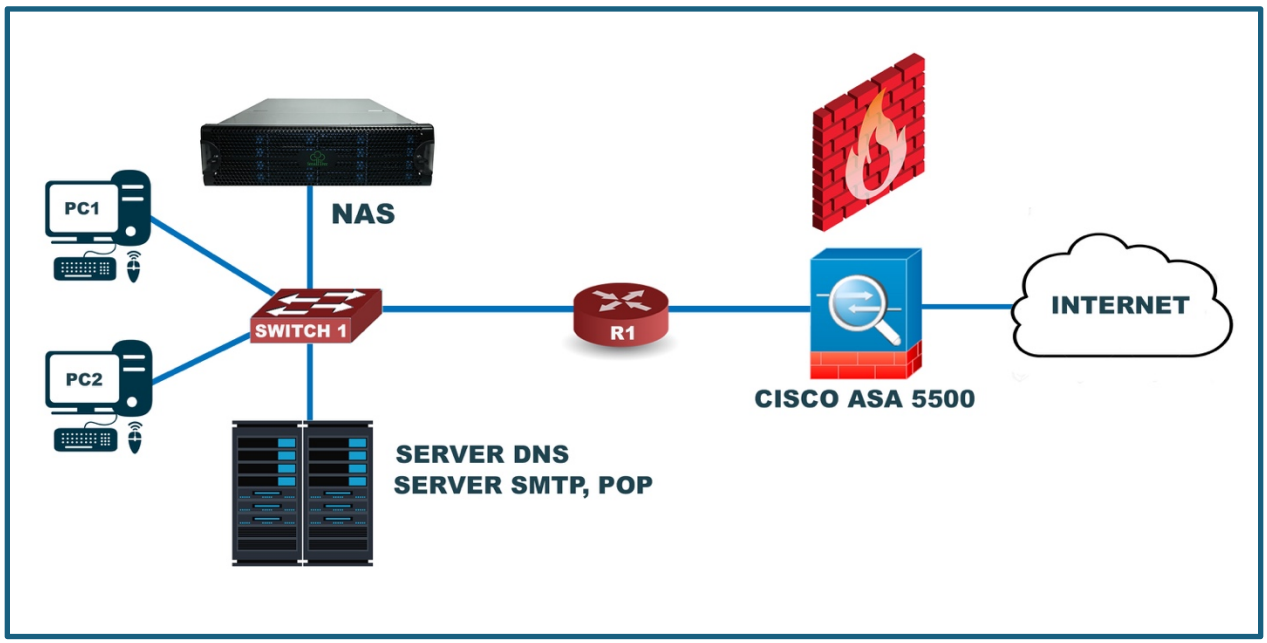


LIST	ACCION	PROTOCOLO	IP ORIGEN	IP DESTINO	PUERTO
101	PERMITIR	TCP	192.168.1.10	CUALQUIERA	80 HTTP
102	DENEGAR	TCP	CUALQUIERA	CUALQUIERA	80 HTTP
103	PERMITIR	TCP	CUALQUIERA	CUALQUIERA	25 SMTP
104	DENEGAR	TCP	CUALQUIERA	200.67.50.1	23 TELNET
104	DENEGAR	TCP	CUALQUIERA	192.168.1.1	23 TELNET

Listas de control de acceso: Es una lista secuencial de instrucciones y/o serie de comandos del IOS que (**permiten o deniegan**) el reenvío o descarte paquetes por parte del Router.

Una ACL es aplicable a todos los protocolos de la capa de aplicación y a las direcciones IP

Las ACL son una herramienta muy potente para controlar el trafico hacia o desde la red. El objetivo es aportar seguridad a la red



El firewall es una de las herramientas de seguridad mas eficaces disponibles para la protección de los usuarios internos de la red, contra amenazas eternas y accesos no autorizados.

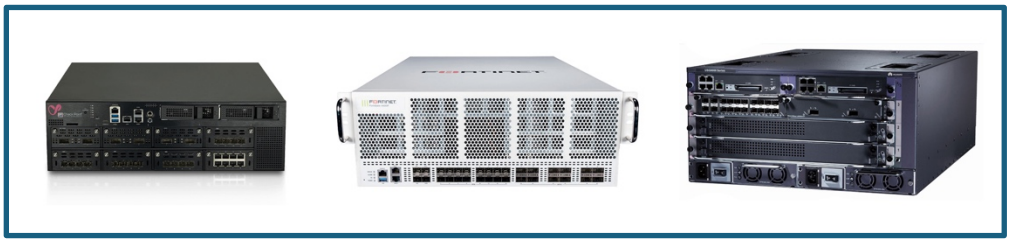
Técnicas y herramientas utilizadas por los Firewalls

- **Filtrado de paquetes:** Deniega o permite el acceso según las direcciones IP
- **Filtrado de aplicaciones:** Deniega o permite el acceso de tipo especifico de aplicaciones conforme a su numero de puerto.
- **Filtrado de URL:** Evita o permite el acceso a sitios web según sus palabras clave o URL especifica.
- **Inspección de paquetes con estado (SPI):** Los paquetes entrantes deben constituir respuestas legitimas a solicitudes de Hosts internos.

FIREWALLS

Firewalls dedicados: Computadoras especializadas que no tienen dispositivos periféricos, son muy rápidos analizando tráficos.

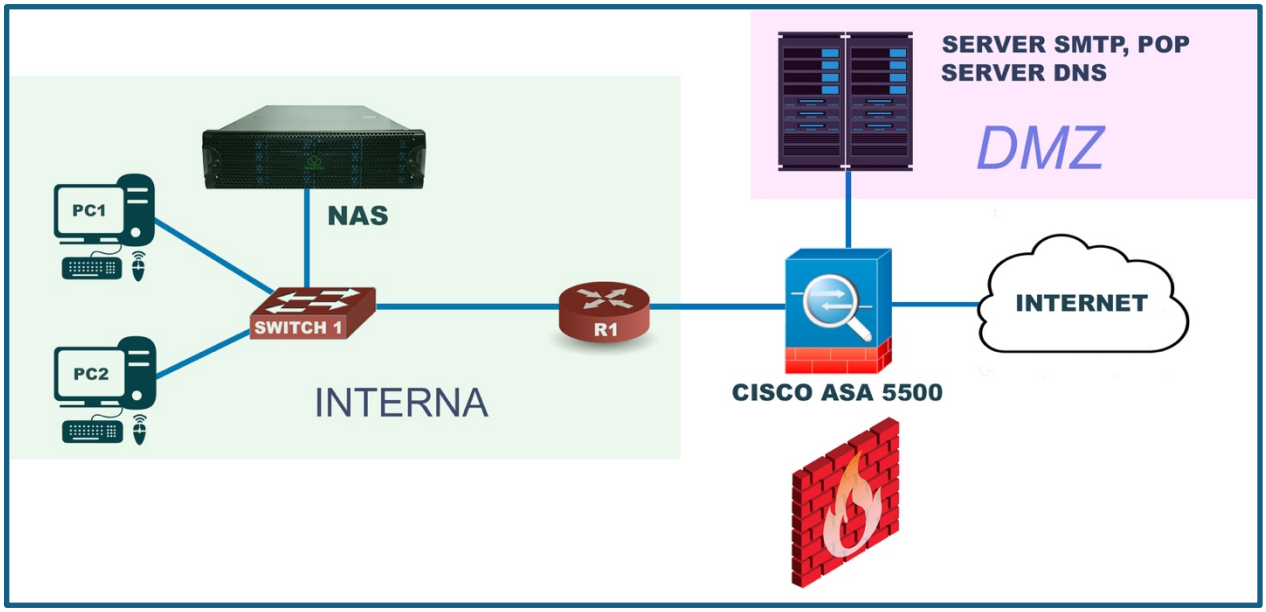
Firewalls server: Aplicación Firewall ejecutada en un sistema operativo como LINUX, WINDOWS. También puede ser software propio del fabricante.



Firewalls Personales: Son aplicaciones propias de los sistemas operativos, las cuales debe revisar que estén activadas.

Firewall softwares: Aplicaciones de terceros que se pueden instalar en los sistemas operativos.

CONFIGURACIONES FIREWALL



Red Interna: Debe estar aislada y protegida, zona en la cual se encuentran las estaciones de trabajo, bases de datos, almacenamiento de archivos y copias de seguridad.

Zona Desmilitarizada: Zona desde la cual se brindar servicios hacia internet, ubicada entre la zona interna e internet.