**OBJETIVO DEL LABORATORIO:** Diseño e implementación de esquemas de líneas preventivas, de detección y recuperación de accesos a recursos sobre la base de un análisis de riesgo para un caso de estudio.

# Actividades

(Los primeros 4 sería necesario que los vesu lado)

1. Leer el Robson Capítuan todos por lo 13
2. <https://docs.netgate.com/pfsense/en/latest/network/index.html> (hay también un PDF de intro a redes en el campus)
3. <https://www.youtube.com/watch?v=OahhshKMM9Y>
4. <https://www.youtube.com/watch?v=6AkKHgdGrHU&t=531s>
5. Hacer el Quizizz de las actividades
6. Plantear el escenario, teniendo en cuenta que la consigna nos pide analizar:

a. ¿Para qué línea de defensa sería útil la implementación de Pfsense?

b. ¿A qué elementos del sistema del escenario ayuda a proteger?

c. ¿De qué amenazas?

1. <https://frre.cvg.utn.edu.ar/pluginfile.php/22593/mod_resource/content/0/UNIDAD_VI-SeguridadyAuditoriaInf/Seguridad-material_complementario.pdf>

NORMAS ISO DE SEGURIDAD (sección 5)

https://www.trusttech.cl/docs/TRUSTTECH\_NCh\_27002\_2022.pdf

1. Hacer el experimento, detallando:

*Los recursos utilizados: generalmente son materiales y herramientas. Se debe detallar el tipo, cantidad y configuraciones de cada uno. Procedimiento: debe detallarse cómo se diseñó la experimentación y los pasos llevados adelante. Luego, deberán realizar pruebas que permitan llevar a cabo el análisis propuesto arriba.*

1. Conclusiones del experimento: Respuestas que surgen luego de la experimentación y del análisis realizado, y que permitirán confirmar (o no) las hipótesis planteadas.
2. Como Administrador de Recursos: ¿qué decisiones podría tomar a partir de lo concluido en la consigna anterior? ¿En qué situaciones sería útil esta herramienta?
3. Hacer la presentación
4. Grabar el video

# Presentación

1 - Investigar y probar la herramienta PFSense. Como guía para la investigación y elaboración de la experiencia se recomienda seguir las siguientes pautas:

1.1 Introducción (1 minuto):

* El planteo del problema a investigar o resolver (situación problemática concreta, en un escenario real o ficticio).
* El objetivo de la experiencia; es decir para qué se realizará.

1.2 Contenido (9 minutos): Es la parte central, en él se deben incluir:

1. **Marco conceptual:** conceptos introductorios que se consideren necesarios para las pruebas a mostrar.
2. **Los recursos utilizados:** generalmente son materiales y herramientas. Se debe detallar el tipo, cantidad y configuraciones de cada uno.
3. **Procedimiento:** debe detallarse cómo se diseñó la experimentación y los pasos llevados adelante. Luego, deberán realizar pruebas que permitan llevar a cabo el análisis propuesto en el punto siguiente. IV.
4. **Aspectos** a analizar en la herramienta, justificando adecuadamente y de manera específica para la herramienta asignada:
   1. ¿Para qué línea de defensa sería útil su implementación?
   2. ¿A qué elementos del sistema ayuda a proteger?
   3. ¿De qué amenazas?
5. Conclusiones del experimento: Respuestas que surgen luego de la experimentación y del análisis realizado, y que permitirán confirmar (o no) las hipótesis planteadas.
6. Como Administrador de Recursos: ¿qué decisiones podría tomar a partir de lo concluido en la consigna anterior? ¿En qué situaciones sería útil esta herramienta?

2 - Elaborar un video de 10 minutos de duración (como máximo), el cual muestre las pruebas y análisis realizados sobre la herramienta asignada.

3 - Proponer actividad

# Cosas que quedan por hacer a día de hoy 21 de junio

* Guion (se puede considerar terminado, falta la política mencionada en el ítem de abajo)
* Pequeña política de seguridad relacionada al escenario para incluir
* Ver cómo desplegar una página bien simple en una red privada cosa de mostrar que un profe puede ver algo que un alumno no (Amilcar y Juli creo que lo están viendo).
* Grabar la demostración
* Presentación (Gamma lo puede hacer rápido, claramente después editándolo para corregir las cosas que dice)
  + https://gamma.app/docs/PF-Sense-Seguridad-de-Red-Eficaz-1m8c2rj6fmrdk4j
* Grabar lo restante

# Introducción

## Escenario

Red de una Escuela Secundaria: cuenta con más de 200 alumnos, 30 profesores y 20 computadoras conectadas a la red en salas de informática, además de equipos en la oficina administrativa, dirección, y secretaría.

**Problemas:**

* Los estudiantes intentan acceder a redes sociales y juegos en horas de clase.
* La red carece de una política clara de seguridad y control de tráfico.
* Las oficinas administrativas necesitan privacidad y protección de datos sensibles.
* No hay control sobre el uso del ancho de banda, saturando las redes.
* No existe una segmentación de red entre estudiantes, profesores y administrativos.

Yo estuve probando el pfsense para hacer ese escenario y lo que está marcado en verde es lo que pude hacer y lo amarillo lo probe un poco.

Pfsense es un firewall basado en el sistema operativo FreeBSD, por eso en la máquina virtual ocupamos ese.

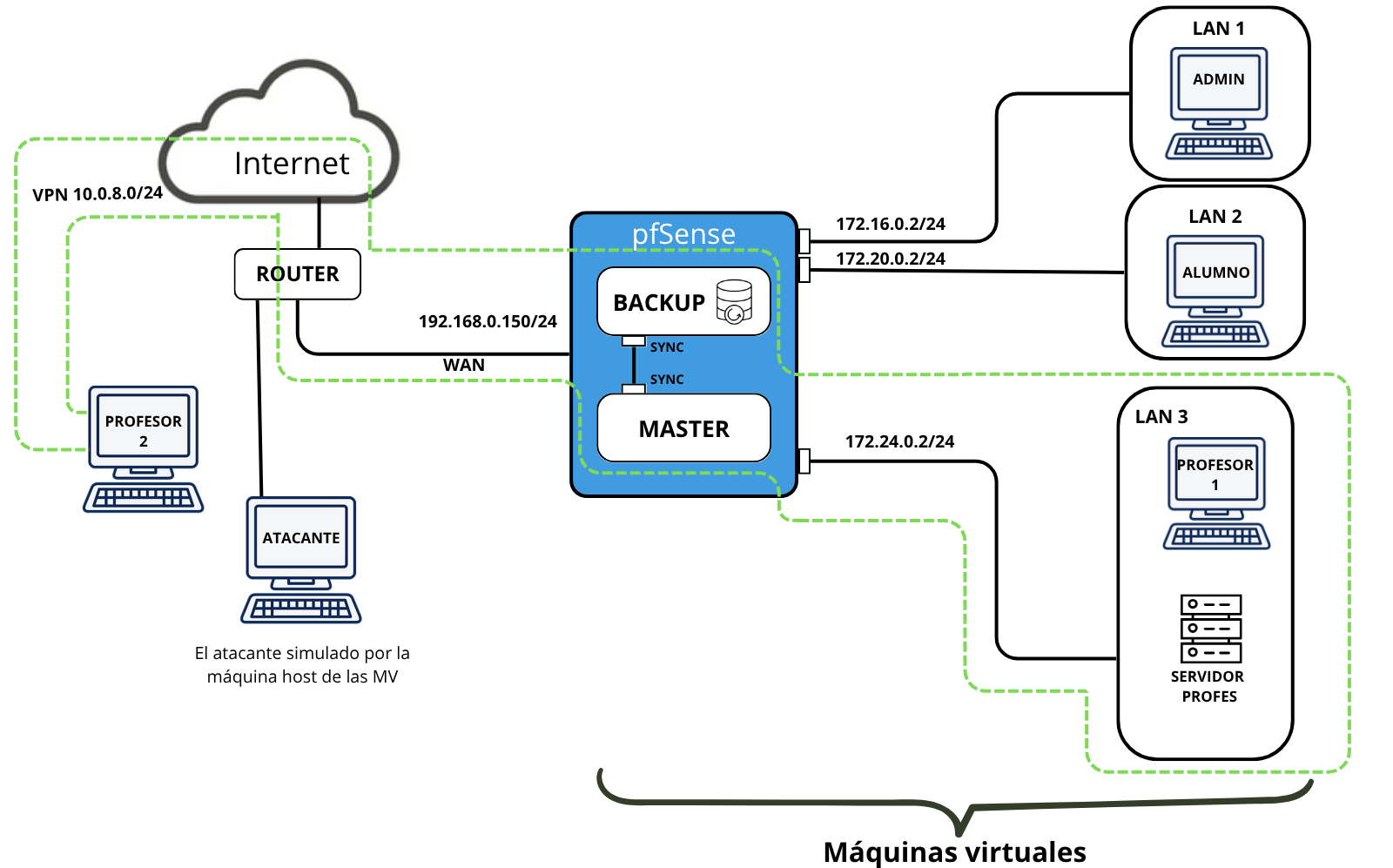
**Soluciones**:

* Restringir el acceso a ciertas páginas web por categoría o dirección IP (para alumnos).
* Limitar el uso de ancho de banda para los estudiantes para evitar saturación de la red.
* Permitir que el personal administrativo y profesores accedan de forma segura desde casa a los sistemas escolares (VPN).
* Configurar un captive portal para que los estudiantes se identifiquen antes de usar Internet. (parece fácil)
* Segmentación de red
* Registro de tráfico(fácil)

Funcionalidades extra:

* Solo los usuarios de admin pueden ingresar a la interfaz de pfsense
  + Identificación de usuarios
* SI SE CAE ALGUNA RED TIENE UN BACKUP
* Bloquear tráfico de ciertos países o regiones para prevenir. podríamos simularlo.
* Notificaciones de eventos. aunque no es seguridad (desde system -> advanced -> notifications)
  + Errores de autenticación
  + Fallos de interfaces
  + Errores de servicio
  + Fallo en backup

[Canva](https://www.canva.com/design/DAGqu6kQ3w8/32Cc87FbWfO5-RfKUCS9Aw/edit?utm_content=DAGqu6kQ3w8&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton)



.

# Contenido

1. Marco conceptual - **Introducción de conceptos sobre la etapa 3**

Existen **cuatro enfoques clásicos para el manejo del riesgo**: prevenir, asumir, reducir o transferir. Cada uno de ellos implica distintas decisiones en cuanto a inversión, control, y tolerancia al impacto. En la práctica, estas estrategias se implementan a través de **controles y contramedidas** que pueden ser tanto técnicos como organizacionales. Su correcta aplicación depende de factores como la plataforma tecnológica utilizada, el grado de distribución del sistema y el nivel de integración de la infraestructura.

Una forma concreta de aplicar estas estrategias es a través del uso de **herramientas de seguridad como pfSense**, un sistema de firewall de código abierto que permite implementar políticas de prevención. Con pfSense se pueden aplicar políticas de seguridad que restrinjan el acceso no autorizado (*prevención*).

* Segunda línea: Para la segunda línea no tiene detección, sólo puede registrar el tráfico.
* Tercera línea: No tiene una función de recuperación, con el Pfsense esclavo lo que hacemos es asegurar una disponibilidad continua previniendo quedarnos sin la protección del firewall, pero no recuperación de datos.

Esta herramienta no solo permite un enfoque más completo en la protección de los sistemas, sino que también proporciona soluciones adaptadas a escenarios reales como el de una red educativa, donde los riesgos son diversos y constantes.

1. Recursos utilizados:

Generalmente son materiales y herramientas. Se debe detallar el tipo, cantidad y configuraciones de cada uno.

* MVs en VirtualBox:
  + PFSense principal con 5 adaptadores de red
    - 1 wan
    - 3 lan
    - 1 sync
  + PFSense para el BACKUP
  + Adaptadores con otra dirección MAC, diferente a la del pfsense original
  + win10 lite con un solo adaptador lan cada uno, cada una de estas máquinas virtuales se conectan a una dirección lan del pfsense principal
* HW dedicado
  + 2 cores, 2gb ram y 50gb ssd
  + 1 core, 2gb ram, 50gb ssd

//buscar la diferencia entre la conecciones con el tema de los MAc

Si el pfSense principal y el de respaldo tuvieran **la misma MAC**, se producirían conflictos en la red, como:

* El tráfico se podría dirigir al pfSense equivocado.
* Se generarían colisiones o errores de ARP (Address Resolution Protocol), donde los dispositivos no sabrían a quién responder.
* En algunos casos, podría interrumpirse el servicio de red o hacer que la alta disponibilidad falle.

1. Procedimiento: Debe detallarse cómo se diseñó la experimentación y los pasos llevados adelante. Luego, deberán realizar pruebas que permitan llevar a cabo el análisis propuesto arriba.

Configuración: Adaptadores de Red en VirtualBox

* **Adaptador 1 (WAN)**
  + **C**onectado a : Red puente (Bridge Adapter)
  + IP obtenida: es asignada por el router doméstico (Ej: 192.168.0.X)
* **2. Adaptador 2 (LAN)** 
  + conectado a: Red Interna (Internal Network)
  + PFSense por defecto configura la interfaz LAN con la IP 192.168.1.1/24.

Esto quiere decir que:

* La dirección IP de la LAN será: 192.168.1.1
* La máscara de subred será: 255.255.255.0
* El rango de IPs disponibles para los clientes LAN será de 192.168.1.2 a 192.168.1.254, siempre que esté habilitado el servidor DHCP (lo está por defecto).

A través de esta interfaz podés:

* Acceder a la interfaz web de administración (http://192.168.1.1)
* Conectar otras máquinas virtuales en red interna (Internal Network) para simular clientes.
* Salir a Internet si está correctamente configurada la interfaz WAN

1. Aspectos analizados
   1. ¿Para qué línea de defensa sería útil su implementación?

En general, PFSense se ubica principalmente en la primera línea de defensa mediante controles técnicos que bloquean amenazas y restringen el acceso.

* 1. ¿A qué elementos del sistema ayuda a proteger?

**Situación del Activo**: En el escenario planteado, los activos en riesgo son principalmente:

* La red escolar: infraestructura tecnológica que conecta las computadoras de alumnos, profesores y personal administrativo.
* La información sensible: como datos personales de alumnos, calificaciones, documentos administrativos, etc
* La reputación institucional: una falla en seguridad también afecta la confianza en la escuela.
  1. ¿De qué amenazas?

**Posibles amenazas:**

* + Acceso no autorizado a recursos o contenido no educativo
  + Riesgo de filtración de datos administrativos
  + Accesos externos inseguros

1. Conclusiones

La implementación de pfSense en el escenario propuesto demostró ser una solución **efectiva, versátil y adecuada** para las necesidades de seguridad de la red de una escuela secundaria. La herramienta permitió abordar de manera concreta los principales problemas identificados: el control del acceso a contenido no autorizado, la segmentación de usuarios según su rol, la protección de datos sensibles del personal administrativo, y la optimización del uso del ancho de banda.

Además, pfSense ofreció funcionalidades complementarias que refuerzan la seguridad y la gestión, como el portal cautivo, el monitoreo del tráfico, el soporte para VPN, la posibilidad de implementar copias de respaldo automáticas (High Availability), y la restricción de acceso a su panel solo a usuarios autorizados.

A pesar de que algunas configuraciones pueden requerir conocimientos técnicos más avanzados, en general, pfSense cumple con su objetivo como solución de firewall y gestión de red. Su uso en este contexto educativo es no solo **conveniente**, sino también **recomendable** por ser una alternativa de código abierto, con alto nivel de personalización y sin costos de licencias

1. Como administrador de Recursos

¿Qué decisiones podría tomar a partir de lo concluido en la consigna anterior?

* **Adoptar pfSense como solución definitiva** para el control de seguridad perimetral de la red, ya que es una herramienta funcional, económica (open source) y adaptable a las necesidades específicas de la escuela.
* **Iniciar una política de segmentación de red permanente**, definiendo subredes diferenciadas para estudiantes, docentes y personal administrativo, aumentando la privacidad y la eficiencia del tráfico.
* **Invertir en capacitación técnica básica** para el personal de IT de la escuela, para garantizar que puedan administrar pfSense de manera autónoma y segura.

¿En qué situaciones sería útil esta herramienta?

* **Protección de datos sensibles** en instituciones que manejan información privada (notas, legajos, informes, etc.).
* **Control de navegación de estudiantes**, bloqueando redes sociales o juegos en horarios escolares.
* **Optimización del ancho de banda**, evitando que el mal uso de la red afecte servicios esenciales como videollamadas o plataformas educativas.
* **Conexiones remotas seguras**, cuando se requiere acceso a la red interna desde ubicaciones externas.
* **Ambientes con necesidad de redundancia**, gracias a su capacidad de alta disponibilidad (HA) en caso de fallos del sistema.
* **Escuelas con recursos limitados**, que necesitan soluciones potentes sin costos de licencias.

Cómo protege PFSense al activo

| **Funcionalidad** | **LDD** | **Activo** | **Cómo lo protege** |
| --- | --- | --- | --- |
| Firewall con reglas de filtrado | 1ra | Red escolar | Permite bloquear el acceso a sitios web no deseados por IP, puerto o categoría, protegiendo la red del mal uso por parte de los alumnos. |
| Limiter / Traffic Shaper | 1ra | Ancho de banda y disponibilidad | Asigna límites de velocidad para ciertos grupos, asegurando que el consumo de red sea justo y evitando que se sature. |
| Segmentación de red con VLAN o interfaces LAN/WAN | 1ra | Información sensible / Red | Separa física o lógicamente a los alumnos de los administrativos para proteger datos internos y evitar accesos cruzados. |
| Captive Portal | 1ra | Control de usuarios | Obliga a los estudiantes a identificarse antes de usar Internet, permitiendo un mejor control y registro. |
| VPN (OpenVPN o IPsec) | 1ra y 3ra | Acceso remoto seguro | Permite que profesores y administrativos accedan a los sistemas desde sus casas sin comprometer la seguridad. |
| Logs de tráfico / monitoreo con ntopng o RRD Graphs | 2da | Registro y análisis de red | Permiten ver quién accede a qué, en qué momento y con qué dispositivo. Ayuda a detectar abusos o fallas. |
| High Availability (HA) | 3ra | Disponibilidad de la red | Si el servidor principal de pfSense falla, uno secundario toma el control automáticamente. Protege la continuidad del servicio. |

# Documentación

## 1 - ¿Qué es PFSense?

El Pfsense es un componente de seguridad que filtra el tráfico de red según reglas predefinidas, el cual el mismo programa realiza la lectura y cumplimiento de los mismos. Es decir es un software basado en el sistema operativo FreeBSD que actúa como firewall y enrutador, brindando funcionalidades avanzadas de seguridad de red. Se utiliza en este entorno como intermediario entre una red privada (LAN) y una red pública (WAN), simulando una estructura real de red empresarial. Además de tener otras funcionalidades que se mencionan posteriormente.

En este caso pfsense se encarga de:

* Controlar tráfico entrante y saliente entre la red LAN (interna) y la red WAN (externa/Internet)
* Bloquear tráfico no autorizado
* Redireccionar puertos (NAT)
* Controlar acceso por DNS (bloqueo de páginas)

## 2 - Estructura de red y entorno de simulación

Para el análisis del entorno de simulación y estructura de red se tuvieron en cuenta los siguientes elementos:

* **Sistema operativo:** FreeBSD 64 bits mediante ISO de pfSense, en una asignación de memoria ram de 2 GB y la utilización de 2 adaptadores red (WAN y LAN)
* **Tipo de entorno: Máquina Virtual - VirtualBox**:

El cual es una representación virtual de una computadora física, que permite ejecutar diferentes sistemas operativos y aplicaciones en un entorno aislado dentro de un mismo hardware permitiendo ejercer la funcionalidad de varias máquinas en un solo computador físico. Se las utiliza debido a sus ventajas como:

* **Mayor eficiencia:** Permiten aprovechar al máximo los recursos del hardware, ejecutando múltiples sistemas operativos y aplicaciones en paralelo.
* **Flexibilidad**: Facilitan la ejecución de diferentes sistemas operativos y aplicaciones, incluso aquellas que no son compatibles con el sistema operativo anfitrión.
* **Ahorro de costos**: Reducen la necesidad de hardware físico, lo que puede disminuir los costos de infraestructura.
* **Seguridad**: Ofrecen un mayor nivel de seguridad, ya que el aislamiento de las máquinas virtuales protege el sistema operativo anfitrión de posibles problemas.
* **Pruebas y desarrollo**: Son ideales para probar software y sistemas operativos en entornos aislados, sin afectar al sistema principal.

## 3 - **Configuración de pfsense en VirtualBox**

Funcionalidades para el control de Redes Locales:

* **Reglas de firewall:** 
  + Permite definir reglas detalladas para permitir o bloquear tráfico en cada interfaz de red (LAN,WAN, etc)
  + Solo se permiten comunicaciones entrantes desde la **interfaz LAN**
  + Todo el tráfico que llega desde interfaces opcionales no definidas es **bloqueado por defecto**
  + Las reglas son **evaluadas en orden secuencial** (de arriba hacia abajo)
  + Se puede restringir el tráfico por dirección IP, puerto, protocolo (TCP/UDP/ICMP), red origen/destino, etc.
* **Nat (Network Address Translation):** 
  + Redireccionamiento de puertos desde la WAN hacia hosts en la LAN.
  + Traducción de direcciones para permitir que varios dispositivos locales compartan una sola IP publica.
* **VPN (Virtual Private Network):** Permite crear túneles seguros entre sitios remotos o usuarios móviles y la red interna por lo cual es ideal para conexión de trabajadores remotos. Es decir permite que personas se conecten a tu red desde cualquier lugar como si estuvieran físicamente allí, de forma segura.
  + Ejemplo: tenés una pequeña empresa y trabajás desde tu casa algunos días. Gracias a la VPN en pfSense, podés conectarte a los archivos y sistemas de tu oficina de forma segura, como si estuvieras sentado ahí.
* **Traffic Shaper (Control de ancho de banda y QoS)**: Se utiliza para priorizar ciertos tipos de tráficos, permitiendo así la limitación de la velocidad de transferencia de datos/paquetes por IP, puerto o protocolo y así prevenir la congestión en la red local
  + Ejemplo: En una red de coworking, un usuario se pone a descargar películas y la conexión se vuelve lenta para todos. Con pfSense podés limitar su velocidad de descarga a 1 Mbps, y reservar más velocidad para quienes usan videollamadas o trabajan online.
* **Captive Portal / Autenticación de usuarios:** Obliga a los usuarios a identificarse para usar internet, es decir por ejemplo si tienes un bar con red local wifi gratuito, en vez de dejar abierto la red, usas captive portal y cuando un cliente se conecta, se le pide que ponga un contraseña o acepte términos, para tener más control y poder evitar abusos en la red local.
  + De modo tal que tiene el siguiente alcance: Control de acceso a la red mediante autenticación local. para el control de acceso web por usuario y contraseña, soporte para vouchers temporales, límite de ancho de banda, tiempo de sesión.