

SAD - U7 Configuración de red con seguridad perimetral

[Descargar estas actividades](#)

Índice

- ▼ Primera parte: DMZ de 3 patas
 - [Referencias y ayuda](#)
 - [Objetivos](#)
 - [Introducción](#)
- ▼ Requisitos del proyecto
 - [Mapa lógico y configuración básica de PFSense \(2 puntos\)](#)
 - [Configuración de la DMZ \(4 puntos\)](#)
 - [Comprobaciones \(4 puntos\)](#)
- ▼ ANEXO I - Configuración de la red en hypervisores
 - [NAT \(no confundir con "NAT Network"\)](#)
 - [Adaptador puente](#)
 - [Red interna](#)
 - [Red solo-anfitrión](#)

Primera parte: DMZ de 3 patas

LEED CADA ENUNCIADO CON ATENCIÓN

- Los nombres de los equipos hosts en VirtualBox, el nombre del sistema cuando lo instaléis, los nombres de usuario, equipo, carpetas, etc. deben ser vuestro nombre+apellido. **En TODAS las capturas debe verse vuestro nombre y apellidos**. Si no se hace así, habrá que repetir TODA la práctica con las capturas adecuadas o no será tenida en cuenta.
- **Responder a todas las preguntas**, si es necesario buscando información en los apuntes del módulo, en los manuales de las aplicaciones, archivos de ayuda y si no se encuentra la solución, incluso en Internet como último recurso.
- En las capturas debéis **MARCAR con círculos o flechas la parte relevante**. Estas capturas deben tener un contexto, es decir, saber de dónde salen. No hagáis mini-capturas ya que no sabré de dónde proviene la información. - Antes de comenzar **podéis hacer un "snapshot" o instantánea de la máquina virtual**. Esto hará que el estado actual de la máquina virtual se guarde y podáis hacer todos los cambios que queráis sin miedo a estropear algo. Ponedle de nombre "Antes de (la acción que vais a hacer)...". Al finalizar, deberéis revertir esta instantánea para volver al estado anterior.
- En general, debéis **comprobar SIEMPRE que los cambios de configuración que hacéis producen el efecto deseado** con el conjunto de pruebas necesario.

Referencias y ayuda

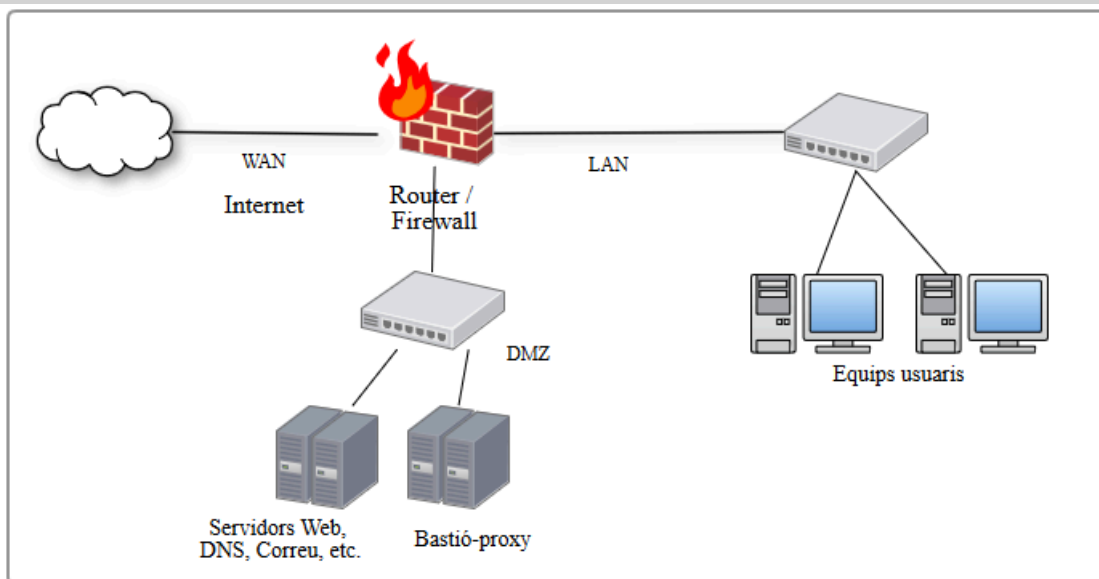
- Descarga PFSense - [PFSense](#)
- Documentación PFSense - [Documentación](#)
- Problemas con paquetes Pfsense - [Problemas](#)
- GNS3 - [Descarga](#)
- Documentación GNS3 - [Documentación](#)
- Guías de uso de GNS3 - [Labs](#)

Objetivos

El objetivo de este proyecto es crear una red más segura, familiarizarse con el concepto de DMZ y explorar las posibilidades de la distribución PFSense/Opnsense.

Introducción

En esta primera parte del proyecto deberéis realizar un montaje de una red DMZ con tres patas.



i pfSense vs OPNsense

- **pfSense/OPNsense** son distribuciones FreeBSD (64 bits) que proporcionan diferentes servicios de red y funcionan como Firewall.
- Se puede configurar desde una interfaz web accesible desde la red LAN.
- Cuando configuramos el firewall, debemos pensar que **las reglas se aplican a las peticiones de inicio de conexión**. Las respuestas se permiten automáticamente si hay una conexión iniciada (porque se ha permitido el paquete de inicio).
- Recordad de **comprobar el hash del fichero descargado** antes de comenzar.
-

✏ Visibilidad de equipos desde el anfitrión

NOTA: Para poder ver desde el equipo anfitrión las máquinas internas, debéis añadir a la tabla de rutas del host anfitrión la red DMZ (192.168.200.0) y si es necesario desde la LAN (192.168.100.0). Su gateway será la IP del pfSense en la red WAN (mirad cuál os asigna). Para añadir una ruta a la tabla de rutas usad el comando:

```
ip route add 192.168.200.0/24 via ip-externa-PFSense
ip route add 192.168.100.0/24 via ip-externa-PFSense
// Para ver la table de rutas y comprobar que se han añadido
ip route
```

Requisitos del proyecto

Mapa lógico y configuración básica de PFSense (2 puntos)

Nuestro firewall será un PFSense con 3 interfaces:

- Una externa conectada vía **red puente** que será 10.100.X.0/16 en el aula o bien quizás 192.168.0.0/24 en casa y que será automática (DHCP).
- Otra de tipo interna para la red LAN (192.168.100.0/24).

- Otra de tipo interna para la DMZ (192.168.200.0/24).

1. Elegid un programa para hacer mapas lógicos de red. Haced el mapa lógico de vuestro montaje. Haced constar:
 - Las direcciones IP de todas las interfaces.
 - Los nombres de los equipos, conteniendo el vuestro.
 - Los servicios que se han puesto en marcha en cada equipo.
2. El ordenador de la red LAN debe poder navegar por Internet.
3. El servicio SSH y el servicio de administración web del Firewall deben estar permitidos en la interfaz WAN. La contraseña del administrador debe ser segura. Una vez hecho, podréis administrar el Firewall desde el equipo físico si lo preferís.

Interfaz de administración

El **PFSense no permite por defecto la configuración web desde la interfaz WAN** y por tanto se debería configurar por una de las interfaces LAN (o sea, por ejemplo desde la máquina virtual Ubuntu Desktop).

Una vez instalado PFSense se puede asignar la configuración de las interfaces y determinar la dirección IP. Desde un equipo de la red LAN se debe abrir un navegador web y abrir la aplicación web de administración de PFSense.

Administración a través de la WAN

No se debe permitir la administración del firewall a través de la WAN. Si se necesita administrar el firewall desde la WAN, se puede hacer a través de una VPN.


En nuestro caso, vamos a permitirlo por la facilidad que nos ofrece a la hora de gestionar la configuración desde nuestro equipo físico, sin necesidad de arrancar una máquina virtual.

Activación de la interfaz de administración a través de la WAN

- El primer paso es configurar una regla de firewall (Firewall -> Rules -> WAN) que permita el tráfico hacia el puerto 443 (HTTPS) y 22 (SSH) desde la WAN.
- A Continuación, si nos fijamos en las reglas de firewall que hay predefinidas, veremos que hay una regla que bloquea el tráfico desde IP's privadas (RFC 1918) a la WAN. Debemos desactivarla. Podemos hacerlo desde la propia regla que bloquea el tráfico o bien desde la configuración de la interfaz WAN, desmarcando la opción

Block private networks .


Generic configuration

 Block private networks

☐

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8) and Carrier-grade NAT addresses (100.64/10). This option should only be set for WAN interfaces that use the public IP address space.

- Si todavía seguimos teniendo problemas para acceder a la aplicación de administración, en entornos donde estemos usando una interfaz en modo Bridge, debemos desactivar la opción "Disable reply-to" desde (Firewall -> Settings -> Advanced) marcando el check correspondiente.

 Disable reply-to

☐ Disable reply-to on WAN rules

With Multi-WAN you generally want to ensure traffic leaves the same interface it arrives on, hence reply-to is added automatically by default. When using bridging, you must disable this behavior if the WAN gateway IP is different from the gateway IP of the hosts behind the bridged interface.

Recuerda que tras cada cambio debes *Guardar los cambios* y *Aplicar los cambios*.

Configuración de la DMZ (4 puntos)

Pondremos un equipo servidor en la DMZ y un cliente en la red local, similar a como se ve en la imagen del comienzo:

1. **Ubuntu Server** con la dirección 10 de la red DMZ, configurado de forma estática NO por DHCP.
 - Con un servicio ssh con banner personalizado.
 - Con un servidor web seguro y no seguro con una página de inicio personalizada.
2. **Un equipo cliente** con la dirección 50 de la red LAN, que puede ser un Ubuntu Desktop.
 - Tendrá el servicio ssh configurado con un banner personalizado.

Personalizado quiere decir que aparecerá vuestro nombre y apellidos en el banner.

1. Actualizad el mapa lógico.
2. Configurad las opciones de Firewall->Rules:
 - El firewall debe **permitir el tráfico iniciado desde la red interna hacia la DMZ**, solo para los servicios que tenga el servidor de la DMZ. Debe llegar la respuesta (esto último es automático en PFSense).
 - También debe **permitir que los servidores de la DMZ accedan tanto a Internet como a la red externa** que es del rango 172.16.101.0/24, y les llegue la respuesta.
 - Se debe **permitir acceder a los servidores de la DMZ desde la red externa, solo para los servicios que tenga el servidor de la DMZ**. NO utilizéis NAT en la interfaz WAN, si no que debéis abrir los puertos necesarios ya que la IP de destino será la del servidor en la DMZ.

No se debe permitir:

- el acceso directo de los equipos de la red interna hacia la red externa (ni internet), para ningún protocolo.
- el acceso directo de los equipos de la red externa (ni internet) a la red interna, para ningún protocolo.
- **No se debe permitir iniciar conexión desde la red DMZ hacia la red interna.**

Comprobaciones (4 puntos)

El objetivo de la práctica es poder comprobar los siguientes puntos (más adelante configuraremos servicios y más limitaciones):

(4 puntos) Hacer comprobaciones que demuestren los puntos que siguen. **En la captura, sin cortes, se debe ver los parámetros IP (la dirección, máscara, tabla de rutas) de la máquina desde la que se está haciendo la prueba**

1. Hacer comprobaciones que demuestren **desde un equipo de la red interna**:
 - Poder hacer **ping, tráfico ssh y acceso a servidores web** hacia el servidor de la DMZ y la respuesta correspondiente.
 - Hacer un mtr (mytraceroute) hacia 8.8.8.8 para ver por dónde pasan los paquetes. Probar a navegar por internet. ¿Se puede?
 - Comprobar si se puede **resolver nombres de dominio** con nslookup www.microsoft.com.
 - Hacer **nmap hacia el servidor de la red DMZ** para ver qué servicios os muestra (solo deberían ser los habilitados en el firewall).
2. Hacer comprobaciones que demuestren **desde un equipo de la red externa** (equipo anfitrión)
 - No poder hacer ping (ni tráfico) desde un equipo de la red externa (anfitrión) hacia los equipos de la red interna. Recordad que primero debéis configurar la tabla de rutas en el anfitrión para que sepa cómo llegar a la red interna y la DMZ.
 - Poder hacer ping (y tráfico ssh y web) hacia la IP del servidor de la DMZ.
 - Hacer nmap hacia el servidor de la red DMZ para ver qué servicios muestra.
3. Hacer comprobaciones que demuestren, **desde un equipo de la DMZ**

- No poder acceder hacia el equipo de la red interna. Se puede probar intentando conectar vía ssh al Desktop interno y hacer ping.
- Hacer un mtr hacia 8.8.8.8 para ver por dónde pasan los paquetes. Probar a navegar por internet.
- Comprobar si se puede resolver nombres de dominio con nslookup www.microsoft.com.
- Probar a navegar por Internet con un navegador en modo texto como lynx. ¿Se puede?
- Hacer nmap hacia el equipo de la red interna para ver qué servicios os muestra.

ANEXO I - Configuración de la red en hipervisores

NAT (no confundir con "NAT Network")

Permite que un equipo virtual tenga acceso a internet de forma fácil. Se crea un router virtual que implementa NAT y traduce las direcciones de los equipos invitados.

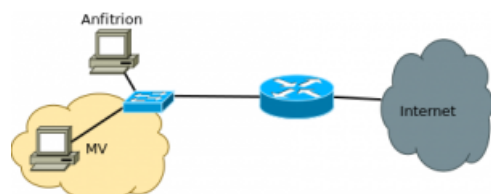


Los equipos invitados no son accesibles directamente desde el anfitrión, pero se puede configurar el reenvío de puertos hacia la máquina invitada y así exponer servicios específicos de la máquina invitada.

Si se necesita que los equipos invitados sean accesibles desde el anfitrión o desde otros equipos de la red, se puede configurar un reenvío de puertos. Por ejemplo, si se quiere acceder a un servidor web en un equipo invitado, se puede configurar un reenvío de puertos para que el tráfico que llegue al puerto 80 del anfitrión se redirija al puerto 80 del equipo invitado.

Adaptador puente

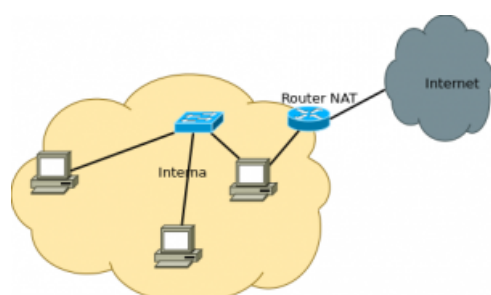
Permite que el equipo invitado tenga acceso a la red física directamente.



Se comportará como si fuera una máquina física más y tendrá una IP de la red física (si existe un servicio DHCP). Se puede acceder desde la máquina anfitrión y desde cualquier equipo de la red física.

Red interna

El equipo invitado se conecta a una red virtual interna. Los equipos invitados pueden comunicarse entre ellos, pero no pueden acceder a la red física ni a internet.



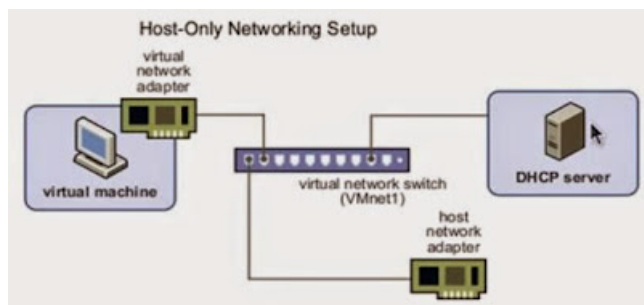
Habría que configurar otro invitado para hacer de router (con una tarjeta en modo puente o NAT), si se quiere dar acceso a internet.

Tampoco se puede acceder al invitado desde el anfitrión.

Red solo-anfitrión

La red solo-anfitrión es una red virtual que se crea en el equipo anfitrión. Los equipos invitados se conectan a esta red y pueden comunicarse entre ellos y con el anfitrión, pero no pueden acceder a la red física ni a internet.

Se crea una nueva interfaz en el equipo físico que se conecta a la red "solo-anfitrión". Así podemos interactuar con los invitados desde el equipo físico, pero sin dar acceso desde la red física.



Hypervisores tipo 1 vs tipo 2

- **Hypervisor tipo 1:** Es un software que se instala directamente en el hardware del servidor y no necesita un sistema operativo anfitrión. Por ejemplo, VMware ESXi, Citrix XenServer.
- **Hypervisor tipo 2:** Es un software que se instala en un sistema operativo anfitrión. Por ejemplo, VirtualBox, VMware Workstation, VMware Player, Microsoft Hyper-V.

Más información en [AWS](#)