

Pfsense (Pluggin TFTP)

miércoles, 25 de octubre de 2023 9:07

Un plugin en pfsense es una extensión de software que se puede agregar para ofrecer funciones adicionales a parte de las que ofrece el propio firewall, esto nos permite ampliar la capacidad de nuestro pfsense según las necesidades que tengamos.

Nosotros vamos a instalar el plugin **TFTP** que sirve para el intercambio de información y archivos entre dos equipos. Funciona a través de UDP y estaca especialmente por ser más sencillo y simple que **FTP**. Utiliza generalmente el **puerto UDP 69** y es común que se use cuando esos dispositivos están conectados dentro de una misma red, en este caso nuestra LAN. No se necesita autenticación, por lo que fuera de esa red podría ser un problema importante de seguridad, pero como lo realizamos dentro de nuestra red, saliendo por un firewall (**pfsense**), no tenemos problema.

-Instalación **TFTP**:

1. Actualizar los repositorios de pfsense:

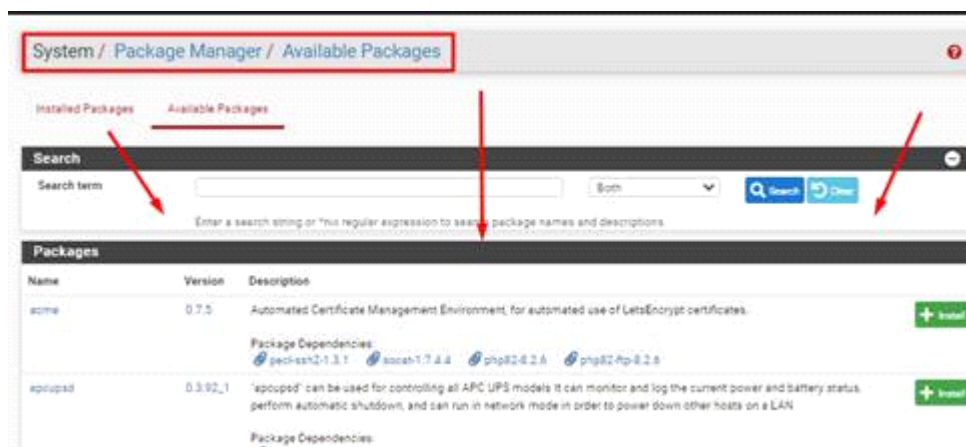
```
WAN (wan)      -> em0      -> v4: 192.168.100.10/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system             14) enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter an option: 13

>>> Updating repositories metadata...
Updating pfSense-core repository catalogue...
```

2. Reiniciar la máquina.
3. Comprobar que después del reinicio, nos aparecen los plugins:



4. Instalar plugin **TFTP**:

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions

Packages

Name	Version	Description
tftpd	0.1.3_4	tftpd installs and runs a TFTP server. We use the versatile tftp-hpa server.

Package Dependencies:
tftp-hpa-5.2_1

Package Installation

```

--
--> NOTICE:

The tftp-hpa port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:

https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:

https://docs.freebsd.org/en/articles/contributing/#ports-contributing
>>> Cleaning up cache... done.
Success

```

5. Comprobamos que se ha instalado correctamente:

Installed Packages Available Packages

Installed Packages

Name	Category	Version	Description
✓ tftpd	ftp	0.1.3_4	tftpd installs and runs a TFTP server. We use the versatile tftp-hpa server.

Package Dependencies:
tftp-hpa-5.2_1

↻ = Update ✓ = Current
 🗑 = Remove ⓘ = Information 🔁 = Reinstall
 ⚠️ Newer version available

Package is configured but not (fully) installed or deprecated

6. Configuración **TFTP**:

- Habilitamos servicio:

Services / TFTP Server / Settings

Settings Files

General Options

Enable TFTP service ☒ Check to enable the TFTP service.

- Asignamos como puerto de escucha del servidor **TFTP** nuestra LAN, ya que se va a usar para la red interna:

TFTP Server Bind IP 192.168.10.1

By default, TFTP server will listen on all local addresses address.

- Solo queremos que se conecten los clientes con IPv4, debido a que el IPv6 lo hemos deshabilitado:

IPv4 Only ☒ Check to allow clients to connect with IPv4 only.

- Permitimos que los clientes también puedan subir archivos al servidor TFTP y tengan permisos de escritura y lectura:

Write Access ☒ Check to allow clients to upload files on the TFTP server.

Logging ☒ Check to log read/write (RRQ/WRQ) requests.

7. Una vez configurado el servidor **TFTP** creamos una regla para permitir el tráfico en la red local a través del puerto 69 (**UDP**):

- Dentro del apartado rules, accedemos a la interfaz local y creamos una regla nueva:

Floating WAN LAN

Rules (Drag to Change Order)							
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway
<input checked="" type="checkbox"/>	4/1.46 MiB	*	*	*	LAN Address	443 80	*
<input type="checkbox"/>	8/7.77 MiB	IPv4 *	LAN net	*	*	*	*
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*

↑ Add

- Especificamos que queremos que la regla sea, en nuestra LAN, mediante el protocolo UDP, con origen LAN net (red local) y destino LAN address (dirección pfsense red local) mediante el puerto 69:

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface LAN
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol UDP
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match LAN net Source Address /
[Display Advanced](#)
 The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match LAN address Destination Address /
Destination Port Range (other) 69 (other) 69
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description REGLA TFTP
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Guardamos y aplicamos cambios.

- Como podemos apreciar la regla se ha creado correctamente:

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/>	7/1.54 MiB	*	*	*	LAN Address	443-80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 UDP	LAN net	*	LAN address	69 (TFTP)	*	none		REGLA TFTP	

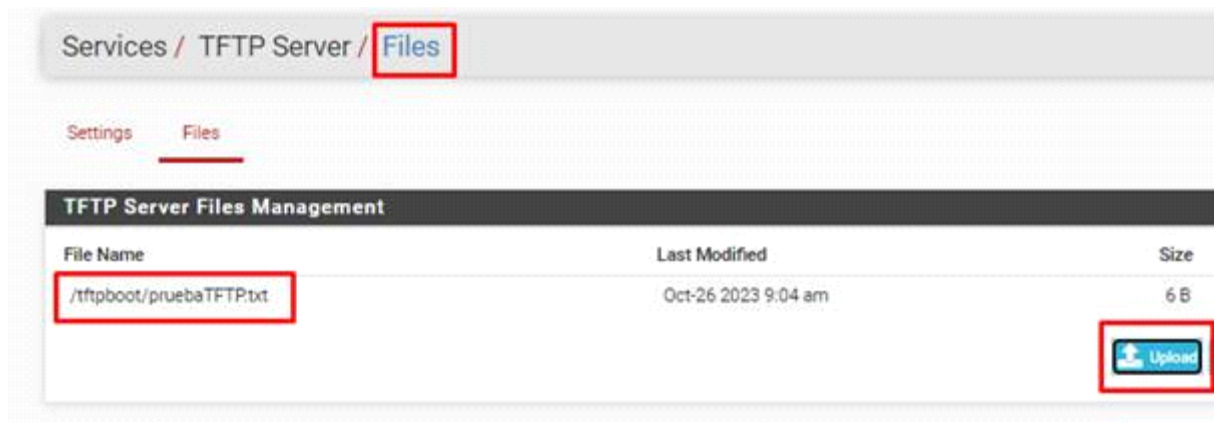
- Subimos un archivo al servidor TFTP, para en el siguiente paso, comprobar que desde un cliente podemos descargar dicho archivo:

Services / TFTP Server / **Files**

Settings Files

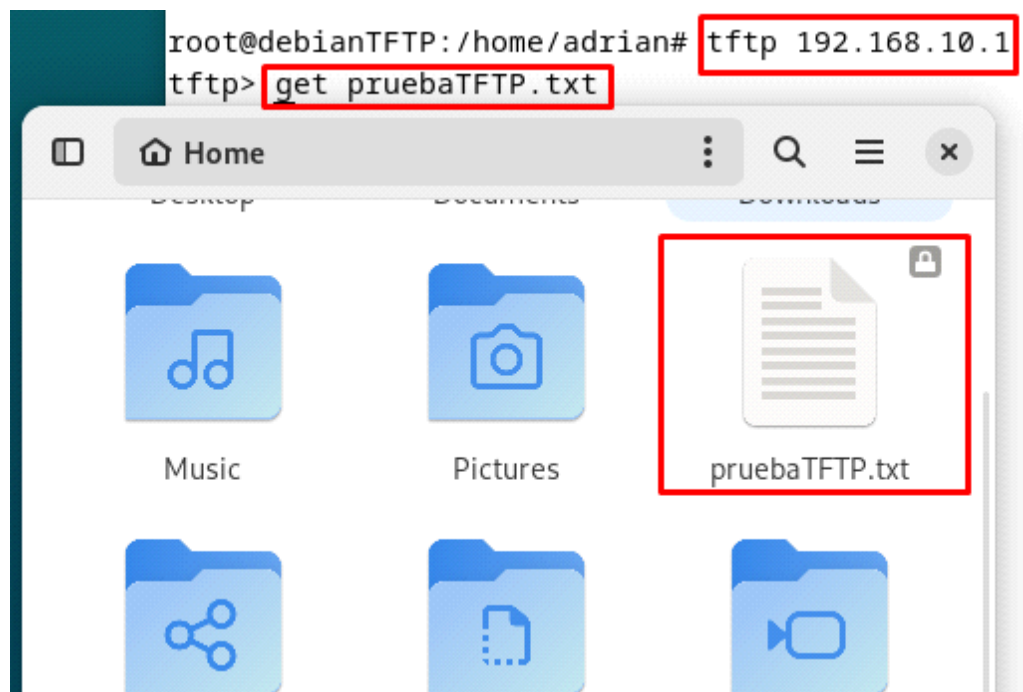
TFTP Server Files Management

File Name	Last Modified	Size
-----------	---------------	------

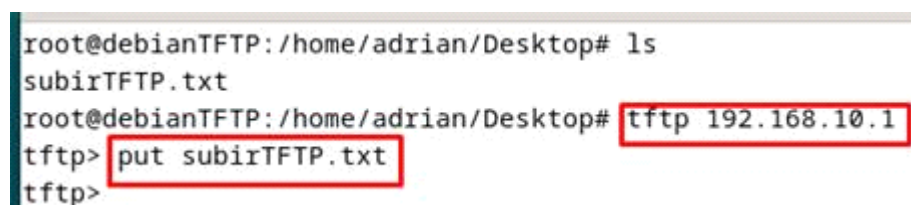


9. Accedemos a un cliente Debian para descargar un archivo a través del servidor TFTP y subir un archivo a dicho servidor, en un Windows también podríamos, pero habría que instalar un programa el cual no parece muy fiable:

- Descargar archivo:



- Subir archivo:



Settings

Files

TFTP Server Files Management

File Name	Last Modified
/tftpboot/subirTFTP.txt	Oct-26 2023 9:34 am
/tftpboot/pruebaTFTP.txt	Oct-26 2023 9:04 am