



Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

Ejercicio – Configuración de un Firewall

Pliego de Descargo

- *Los ejercicios y conocimientos contenidos en el Módulo 5021, Incidentes de Ciberseguridad, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos.***
- *Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.*



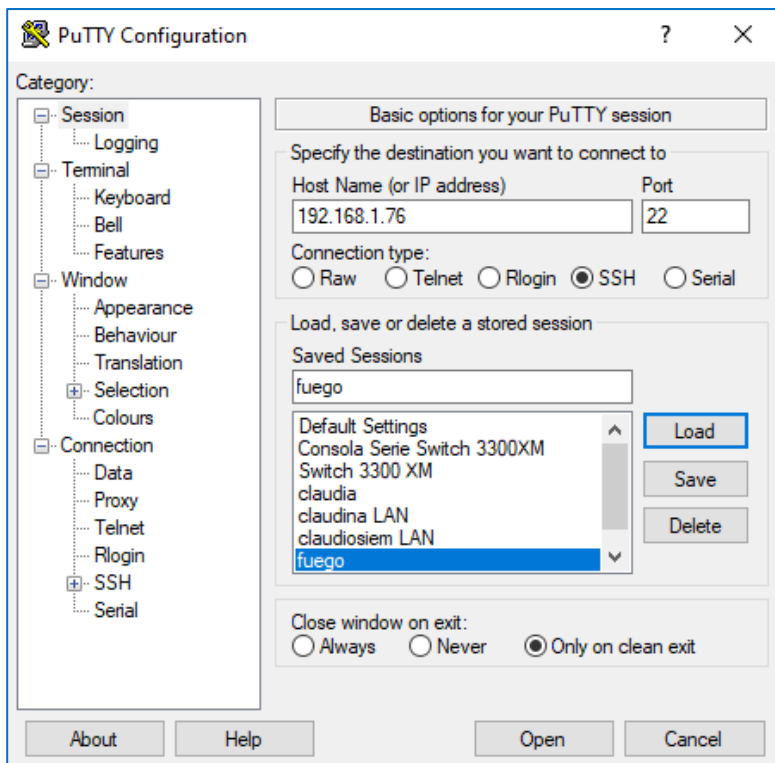
Índice de contenidos

1. Instalación y Configuración del Firewall
2. Prueba de Bloqueo de Accesos

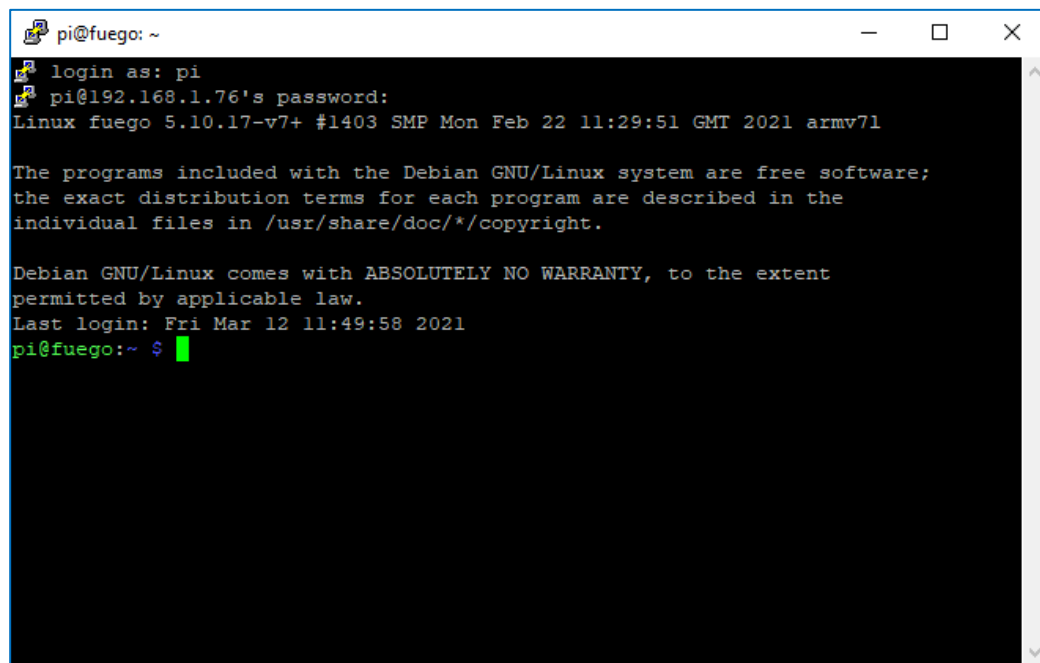


1. Instalación y Configuración del Firewall

Conexión al Host “fuego”

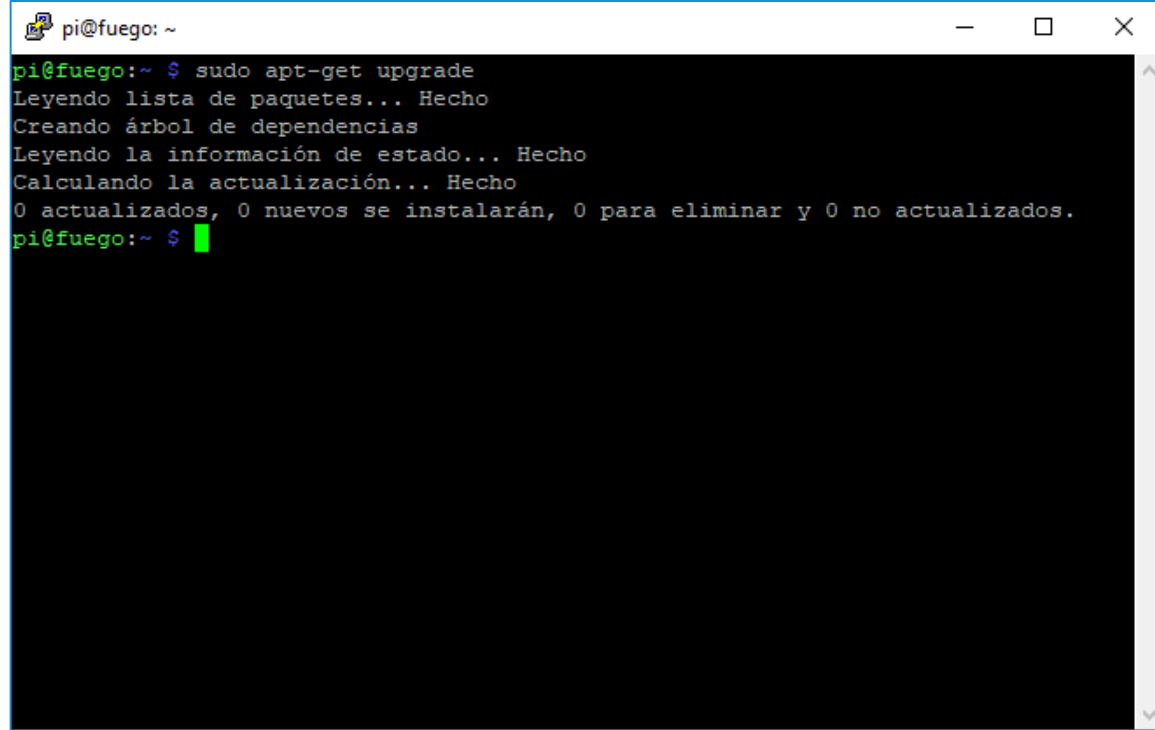


- Fuego es una Raspberry Pi 3B+ con Raspbian recién instalado.



Actualización de Raspbian

- En primer lugar, efectuamos un upgrade del SW de Raspbian.



```
pi@fuego: ~  
pi@fuego:~ $ sudo apt-get upgrade  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Calculando la actualización... Hecho  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
pi@fuego:~ $
```

Instalación de UFW – Uncomplicated Firewall - Ubuntu

- Instalamos Uncomplicated FireWall sobre Raspbian.
- Se trata de un SW de Firewall desarrollado por la Comunidad UBUNTU.
- Está escrito en Python.

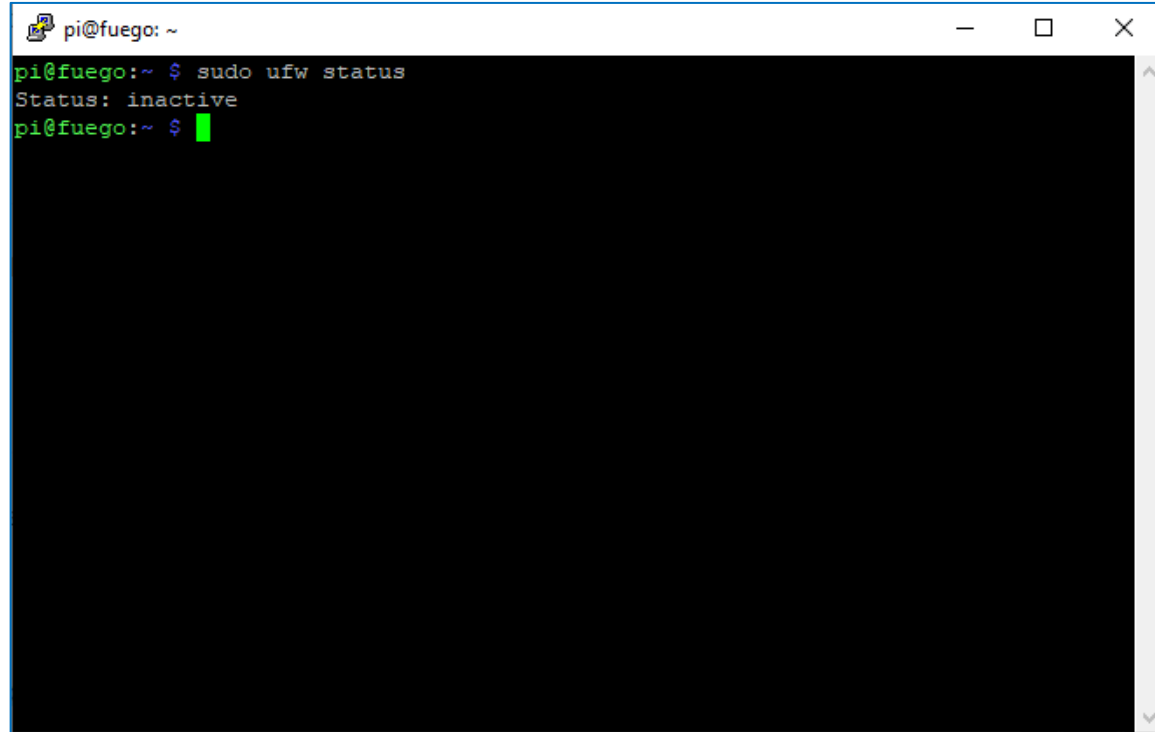
```
pi@fuego: ~  
pi@fuego:~ $ sudo apt install ufw  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  ufw  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 164 kB de archivos.  
Se utilizarán 852 kB de espacio de disco adicional después de esta operación.  
Des:1 http://ftp.cica.es/mirrors/Linux/raspbian/raspbian buster/main armhf ufw a  
11 0.36-1 [164 kB]  
Descargados 164 kB en 1s (313 kB/s)  
Preconfigurando paquetes ...  
Seleccionando el paquete ufw previamente no seleccionado.  
(Leyendo la base de datos ... 98610 ficheros o directorios instalados actualment  
e.)  
Preparando para desempaquetar .../archives/uw_0.36-1_all.deb ...  
Desempaquetando uw (0.36-1) ...  
Configurando uw (0.36-1) ...  
  
Creating config file /etc/uw/before.rules with new version  
  
Creating config file /etc/uw/before6.rules with new version
```

Verificación de Estado del Cortafuegos

- Verificamos el estado del Firewall con el comando:

```
sudo ufw status
```

- Al estar recién instalado, debería estar apagado.



```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: inactive  
pi@fuego:~ $
```


Configuración Básica del Firewall

Antes de habilitar el cortafuegos, ejecutaremos los siguientes comandos, para establecer una configuración básica, que es típica de cualquier servidor:

- `sudo ufw default deny incoming`. Por defecto, bloqueo del tráfico entrante en todos los puertos, a excepción de los que se abran con sentencias posteriores a ésta.
- `sudo ufw default allow outgoing`. Por defecto, apertura del tráfico saliente desde todos los puertos.
- `sudo ufw allow 1194/udp`. Este puerto deberá estar abierto si se va a usar una VPN con el protocolo OpenVPN, por ejemplo.
- `sudo ufw allow 80/tcp`. Abrimos el puerto necesario para que funcione un servidor web instalado en la máquina.
- `sudo ufw allow 443/tcp`. Abrimos también el puerto que utilizará el servidor web si empleamos el protocolo seguro https.
- `sudo ufw allow 22/tcp`. Esta es la sentencia de apertura más importante, puesto que en la mayoría de los casos los hosts se administran en remoto, y este es el puerto que precisa el protocolo SSH para abrir una sesión segura (*Secure Shell*). Si activamos el cortafuegos con las sentencias anteriores pero olvidamos abrir este puerto, dejaremos la máquina totalmente aislada en términos de sesiones y habrá que ir físicamente a la consola del host para reactivar este acceso.

Configuración Básica del Firewall

- Ejecutamos los comandos en cuestión y verificamos sus respuestas.

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: inactive  
pi@fuego:~ $ sudo ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
pi@fuego:~ $ sudo ufw default allow outgoing  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
pi@fuego:~ $ sudo ufw allow 1194/udp  
Rules updated  
Rules updated (v6)  
pi@fuego:~ $ sudo ufw allow 80/tcp  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
pi@fuego:~ $ sudo ufw allow 443/tcp  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
pi@fuego:~ $ sudo ufw allow 22/tcp  
Rules updated  
Rules updated (v6)  
pi@fuego:~ $
```

Arranque y Parada del Cortafuegos

- Una vez programadas las reglas, se puede activar el cortafuegos (*enable*) y desactivarlo (*disable*) en cualquier momento para cambiar la configuración:

```
sudo ufw enable
```

- Tras el arranque, es conveniente comprobar de nuevo su estado:

```
sudo ufw status
```

- La situación en la que dejemos el cortafuegos prevalecerá tras un re arranque de máquina, tanto en términos de activación como en términos de reglas.
- **NOTA.** Obsérvese que antes de arrancar el cortafuegos se nos avisa de que tengamos cuidado con las reglas para no bloquear nuestro propio acceso a la máquina, como comentábamos en el paso anterior.

Arranque y Parada del Cortafuegos

- Ejecutamos los comandos en cuestión y verificamos sus respuestas.

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw enable  
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y  
Firewall is active and enabled on system startup  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
80/tcp ALLOW Anywhere  
443/tcp ALLOW Anywhere  
1194/udp ALLOW Anywhere  
22/tcp ALLOW Anywhere  
80/tcp (v6) ALLOW Anywhere (v6)  
443/tcp (v6) ALLOW Anywhere (v6)  
1194/udp (v6) ALLOW Anywhere (v6)  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $ sudo ufw disable  
Firewall stopped and disabled on system startup  
pi@fuego:~ $
```

Modificación de Reglas en Caliente

- Cuando el cortafuegos está levantado y funcionando, se puede modificar la tabla de reglas en vivo, en caso de que se desee cambiar algún detalle del comportamiento.
- Habrá que tener mucho cuidado al utilizar esta funcionalidad, pues también nos puede dejar sin conexión al host, pero en esta ocasión no recibiremos avisos previos de ningún tipo.

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: inactive  
pi@fuego:~ $ sudo ufw enable  
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y  
Firewall is active and enabled on system startup  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
80/tcp ALLOW Anywhere  
443/tcp ALLOW Anywhere  
1194/udp ALLOW Anywhere  
22/tcp ALLOW Anywhere  
80/tcp (v6) ALLOW Anywhere (v6)  
443/tcp (v6) ALLOW Anywhere (v6)  
1194/udp (v6) ALLOW Anywhere (v6)  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $ sudo ufw delete allow 1194/udp  
Rule deleted  
Rule deleted (v6)  
pi@fuego:~ $
```

Modificación de Reglas en Caliente

- Verificamos que la regla en cuestión ha sido eliminada de la tabla del cortafuegos.

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
80/tcp ALLOW Anywhere  
443/tcp ALLOW Anywhere  
22/tcp ALLOW Anywhere  
80/tcp (v6) ALLOW Anywhere (v6)  
443/tcp (v6) ALLOW Anywhere (v6)  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $
```



2. Prueba de Bloqueo

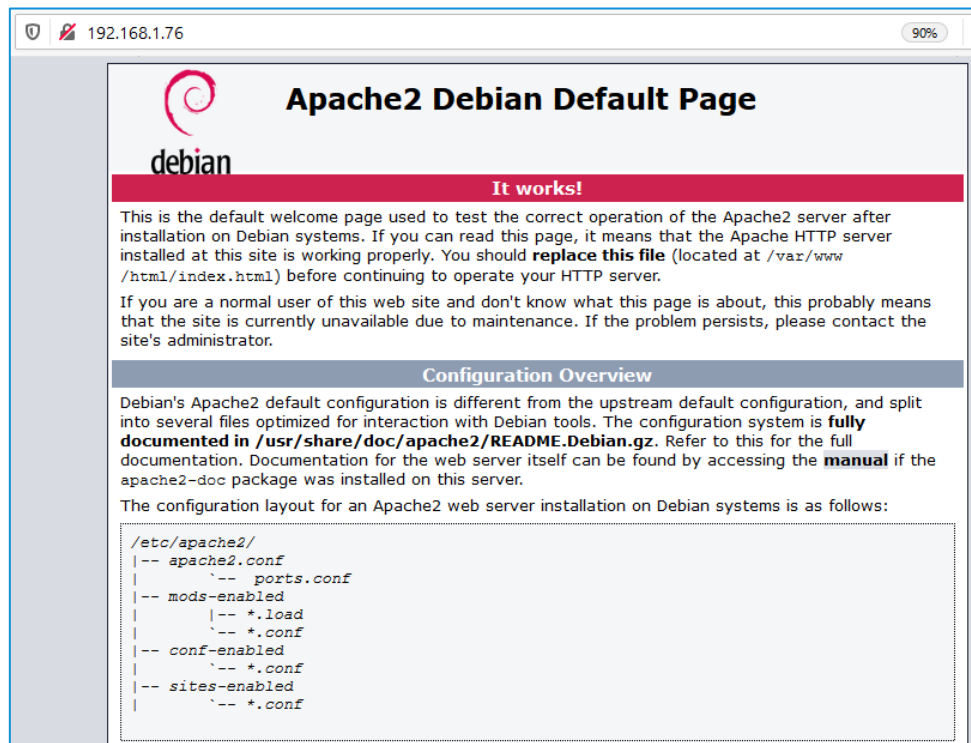
Prueba de Bloqueo del Acceso al Servidor Web

- Instalamos un servidor Apache para efectuar la prueba de bloqueo:

```
sudo apt update
```

```
sudo apt install apache2
```
- Comprobamos el status:

```
sudo systemctl status apache2
```
- Comprobamos que se visualiza la página inicial de Apache introduciendo la Dirección IP del host en el Navegador de Internet del PC.



Prueba de Bloqueo del Acceso al Servidor Web

- Bloqueamos los puertos de acceso HTTP (80) y HTTPS (443) e intentamos acceder al servidor web de nuestro host 192.168.1.76 desde un PC conectado a la misma LAN.
- Como resultado de este bloqueo, se observa que el servidor web ya no está accesible (ver página siguiente).

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
80/tcp ALLOW Anywhere  
443/tcp ALLOW Anywhere  
22/tcp ALLOW Anywhere  
80/tcp (v6) ALLOW Anywhere (v6)  
443/tcp (v6) ALLOW Anywhere (v6)  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $ sudo ufw delete allow 80/tcp  
Rule deleted  
Rule deleted (v6)  
pi@fuego:~ $ sudo ufw delete allow 443/tcp  
Rule deleted  
Rule deleted (v6)  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
22/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $
```

Prueba de Bloqueo del Acceso al Servidor Web

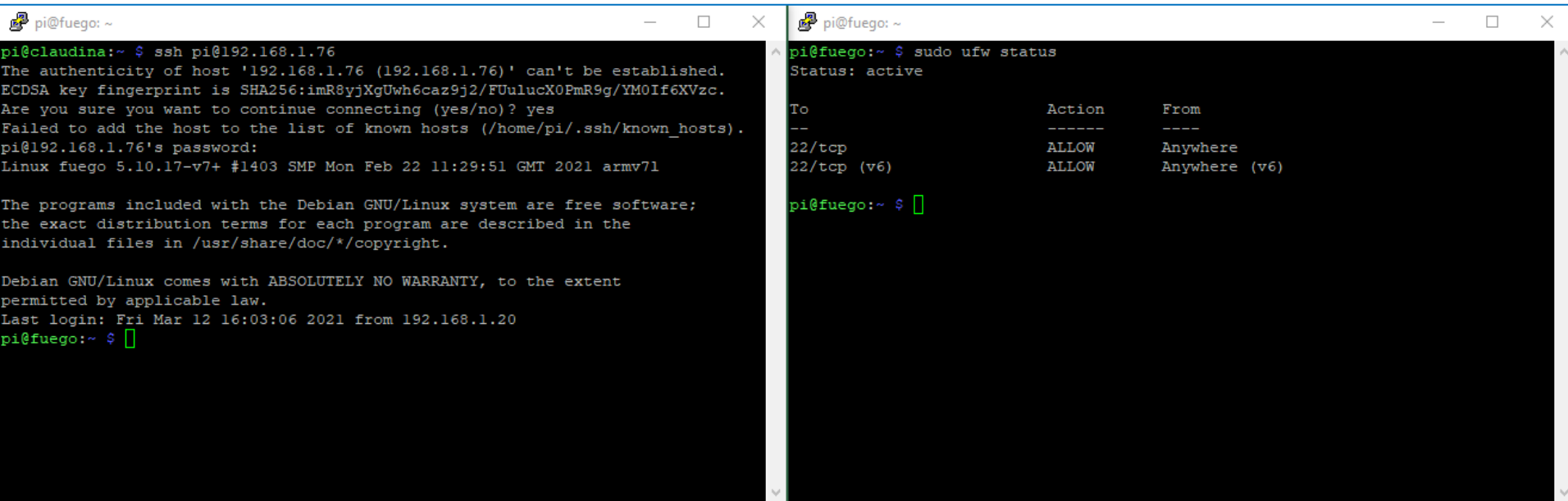


Prueba de Bloqueo del Acceso SSH

- Probamos ahora a bloquear el puerto 22 para cerrar el acceso SSH.
- **ATENCIÓN:** esta acción dejará el host incomunicado para administración a través de la red, pues impedirá abrir sesiones en remoto. El resto de las funciones y comunicaciones seguirán operando normalmente, salvo que también se estén filtrando en el firewall.
- Para recuperar la normalidad, el técnico tendrá que desplazarse físicamente al Data Center, entrar en el host a través de su consola, y cambiar las reglas del firewall.

Prueba de Bloqueo del Acceso SSH

- Antes de bloquear el acceso por el puerto 22, comprobamos que se puede abrir una sesión ssh desde el host “claudina”, conectado a la misma LAN.



```
pi@fuego: ~  
pi@claudina:~ $ ssh pi@192.168.1.76  
The authenticity of host '192.168.1.76 (192.168.1.76)' can't be established.  
ECDSA key fingerprint is SHA256:imR8yJXgUwh6caz9j2/FUulucX0PmR9g/YM0If6XVzc.  
Are you sure you want to continue connecting (yes/no)? yes  
Failed to add the host to the list of known hosts (/home/pi/.ssh/known_hosts).  
pi@192.168.1.76's password:  
Linux fuego 5.10.17-v7+ #1403 SMP Mon Feb 22 11:29:51 GMT 2021 armv7l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Mar 12 16:03:06 2021 from 192.168.1.20  
pi@fuego:~ $  
  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
22/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $
```

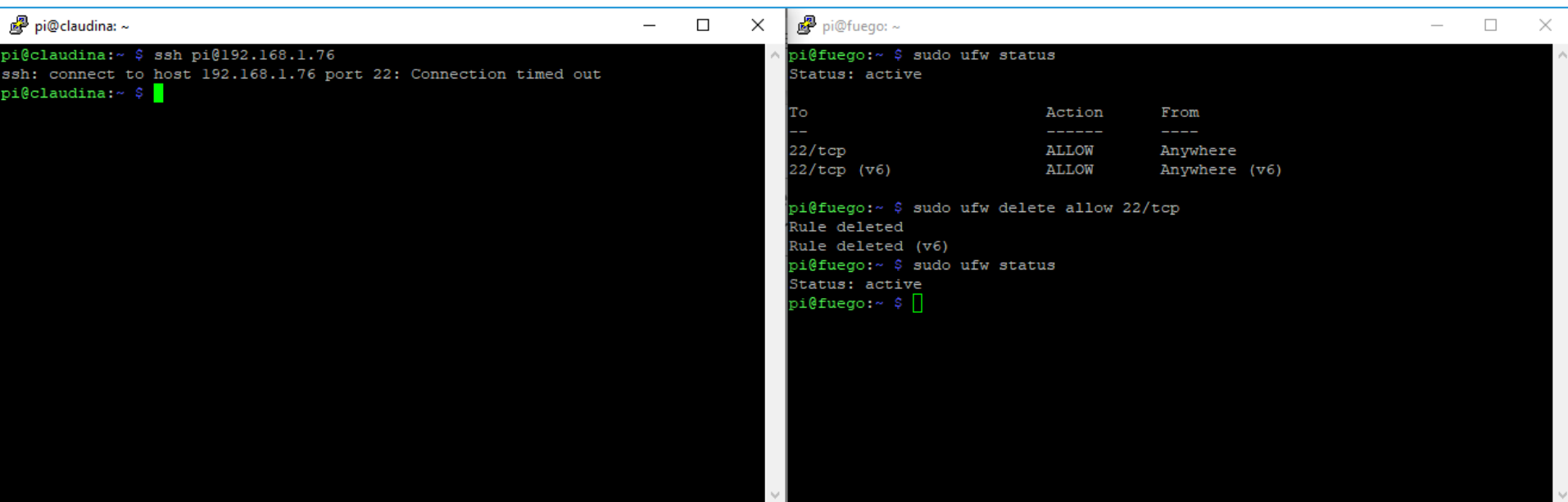
Prueba de Bloqueo del Acceso SSH

- Bloqueamos el acceso por el puerto 22, borrando la regla que permite entrar por dicho puerto.
- Comprobamos en el status que la tabla se ha quedado ya sin ninguna regla de paso, mientras que el cortafuegos sigue activo.
- La máquina está aislada para ssh, además de para la web.

```
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
22/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $ sudo ufw delete allow 22/tcp  
Rule deleted  
Rule deleted (v6)  
pi@fuego:~ $ sudo ufw status  
Status: active  
pi@fuego:~ $
```

Prueba de Bloqueo del Acceso SSH

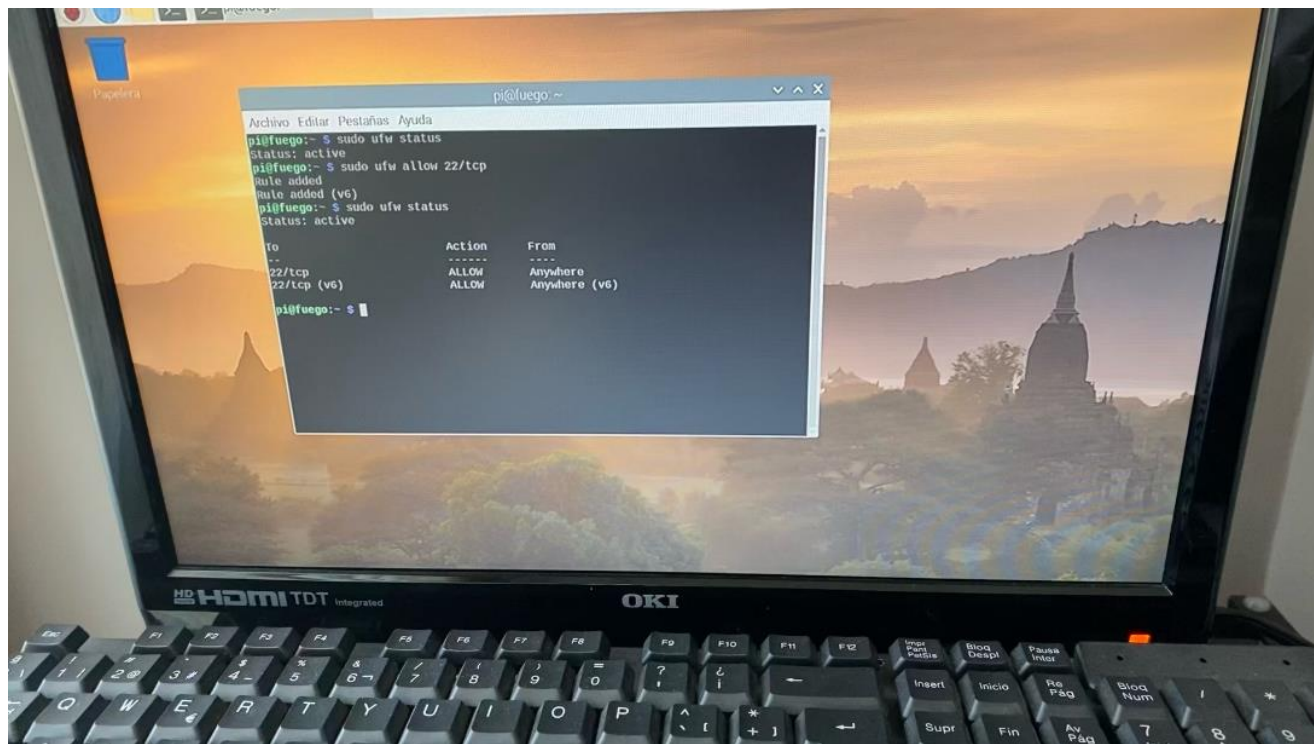
- Si intentamos entrar a “fuego” desde “claudina” por ssh, vemos que ya no es posible y que el comando temporiza y aborta. La máquina ha quedado aislada.



```
pi@claudina: ~  
pi@claudina:~ $ ssh pi@192.168.1.76  
ssh: connect to host 192.168.1.76 port 22: Connection timed out  
pi@claudina:~ $  
  
pi@fuego: ~  
pi@fuego:~ $ sudo ufw status  
Status: active  
  
To Action From  
--  
22/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
  
pi@fuego:~ $ sudo ufw delete allow 22/tcp  
Rule deleted  
Rule deleted (v6)  
pi@fuego:~ $ sudo ufw status  
Status: active  
pi@fuego:~ $
```

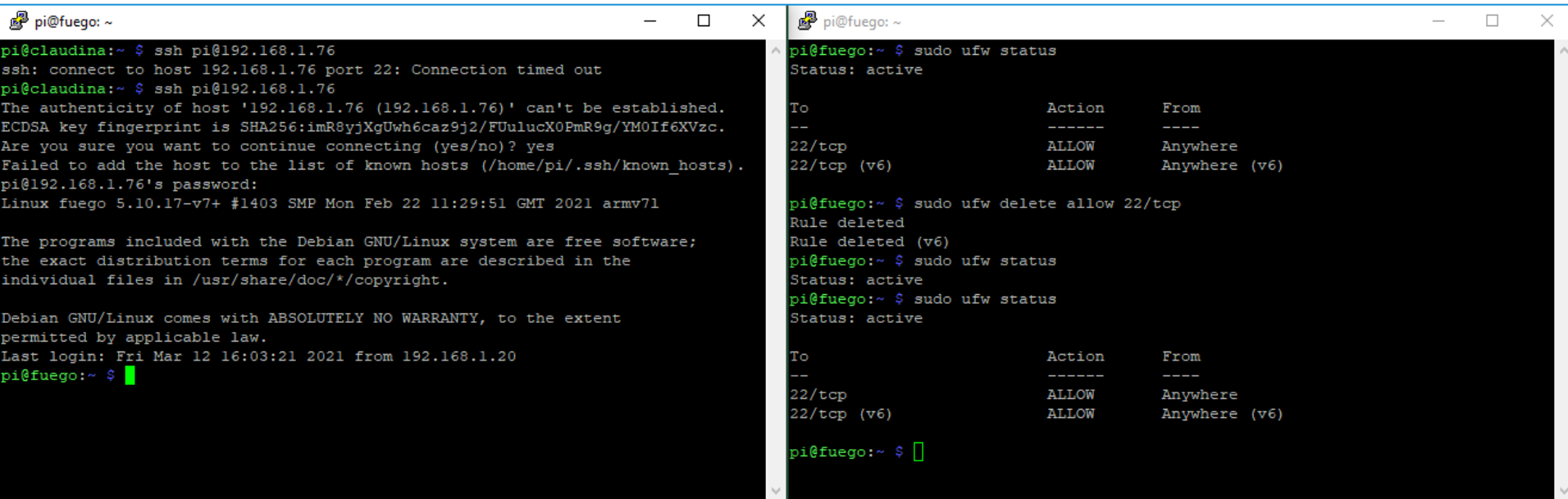
Prueba de Bloqueo del Acceso SSH

- Añadimos de nuevo la regla de paso al firewall desde la consola física de la máquina en el Data Center.



Prueba de Bloqueo del Acceso SSH

- Volvemos a intentar conectarnos por ssh desde “claudina” y comprobamos que se ha recuperado el acceso a “fuego”.



The image shows two terminal windows side-by-side. The left window is titled 'pi@fuego: ~' and shows an SSH connection attempt from 'claudina' to '192.168.1.76'. The connection times out, and the user is prompted to add the host to the known hosts list. The user accepts, and the terminal displays the SSH fingerprint and a warning about the Debian GNU/Linux system. The right window is also titled 'pi@fuego: ~' and shows the user running 'sudo ufw status'. The output shows that the firewall is active and allows traffic on port 22/tcp from anywhere. The user then runs 'sudo ufw delete allow 22/tcp', which deletes the rule. Finally, the user runs 'sudo ufw status' again, and the output shows that the firewall is still active but the rule for port 22/tcp has been removed.

```
pi@claudina:~ $ ssh pi@192.168.1.76
ssh: connect to host 192.168.1.76 port 22: Connection timed out
pi@claudina:~ $ ssh pi@192.168.1.76
The authenticity of host '192.168.1.76 (192.168.1.76)' can't be established.
ECDSA key fingerprint is SHA256:imR8yXgUwh6caz9j2/FUulucX0PmR9g/YM0If6XVzc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/pi/.ssh/known_hosts).
pi@192.168.1.76's password:
Linux fuego 5.10.17-v7+ #1403 SMP Mon Feb 22 11:29:51 GMT 2021 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 12 16:03:21 2021 from 192.168.1.20
pi@fuego:~ $
```

```
pi@fuego:~ $ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

pi@fuego:~ $ sudo ufw delete allow 22/tcp
Rule deleted
Rule deleted (v6)
pi@fuego:~ $ sudo ufw status
Status: active
pi@fuego:~ $ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

pi@fuego:~ $
```


Bibliografía

- <https://help.ubuntu.com/community/UFW>
- <https://wiki.ubuntu.com/UncomplicatedFirewall>