

ubuntu

Proteger GNU/Linux con la configuración del cortafuegos de sistema ufw

Alfredo Abad
PARP412-Cortafuegos-ufw.pptx
UA: 13-ago-2018

Basado en <https://www.atareao.es/ubuntu/protege-ubuntu-en-redes-publicas-con-cortafuegos/>

Objetivo de la práctica y materiales necesarios

- **Objetivos:**
 - Comprender la función básica de un cortafuegos
 - Gestionar ufw, el cortafuegos básico incluido en GNU/Linux
 - Aprender a crear reglas sencillas
- **Materiales necesarios:**
 - Sistema GNU/Linux
 - Otros sistemas para la realización de pruebas de conexión remota
- Se trata de estudiar ufw/gufw para que configures algunas reglas sencillas para el cortafuegos de un sistema Linux
 - Prueba a realizar algunas de las conexiones permitidas/prohibidas para que queden reflejadas en la documentación de la práctica

El cortafuegos de Ubuntu

- En Ubuntu y derivados hay un cortafuegos instalado por defecto (iptables)
 - Que puede ser gestionado por una sencilla aplicación: Uncomplicated Firewall (ufw)
 - También dispone de una interfaz gráfico (Linux Desktop): Gufw

OPERACIÓN

Acciones iniciales

- Por defecto ufw no está activado, pero con frecuencia será necesario protegerse del exterior activándolo
 - **sudo ufw enable**
- Se puede comprobar el estado del firewall con
 - **sudo ufw status verbose**

```

Terminal Archivo Editar Ver Buscar Terminal Ayuda
lorenzo ~$ sudo ufw status verbose
[sudo] password for lorenzo:
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), deny (enrutados)
Perfiles nuevos: skip

Hasta      Acción      Desde
-----
Anywhere   ALLOW IN    192.168.1.0/24
22         ALLOW IN    Anywhere
22 (v6)     ALLOW IN    Anywhere (v6)

Anywhere   ALLOW OUT    Anywhere
Anywhere (v6) ALLOW OUT    Anywhere (v6)

lorenzo ~$

```

Visualizar las reglas del cortafuegos (detalle): sudo ufw show raw

```

Terminal
lorenzo ~$ sudo ufw show raw
IPV4 (raw):
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source destination
 39183 55177550 ufw-before-logging-input all -- * * 0.0.0.0/0 0.0.0.0/0
 39183 55177550 ufw-before-input all -- * * 0.0.0.0/0 0.0.0.0/0
    3 234 ufw-after-input all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-after-logging-input all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-reject-input all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-track-input all -- * * 0.0.0.0/0 0.0.0.0/0

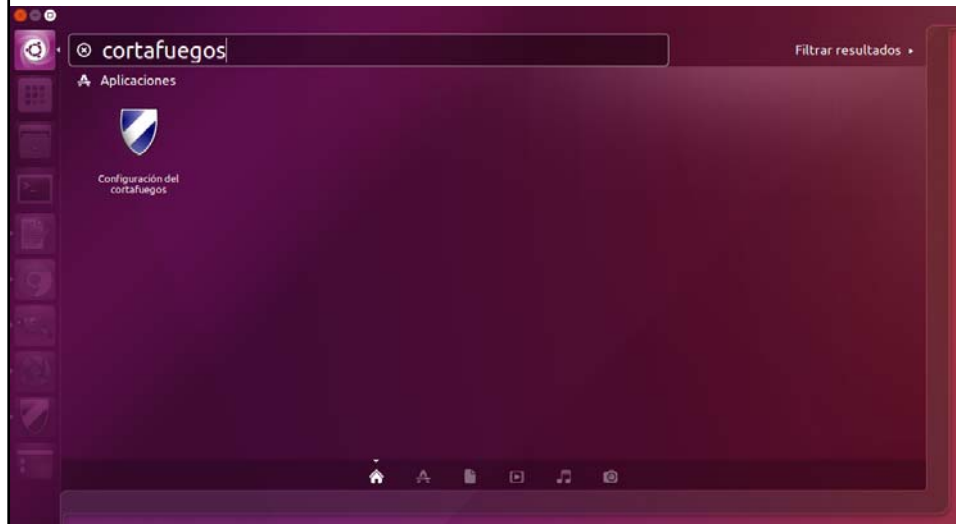
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target prot opt in out source destination
    0 0 DOCKER-ISOLATION all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 DOCKER all -- * docker0 0.0.0.0/0 0.0.0.0/0
    0 0 ACCEPT all -- * docker0 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED
    0 0 ACCEPT all -- docker0 !docker0 0.0.0.0/0 0.0.0.0/0
    0 0 ACCEPT all -- docker0 docker0 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-before-logging-forward all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-before-forward all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-after-forward all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-after-logging-forward all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-reject-forward all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-track-forward all -- * * 0.0.0.0/0 0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target prot opt in out source destination
 23708 1456052 ufw-before-logging-output all -- * * 0.0.0.0/0 0.0.0.0/0
 23708 1456052 ufw-before-output all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-after-output all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-after-logging-output all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-reject-output all -- * * 0.0.0.0/0 0.0.0.0/0
    0 0 ufw-track-output all -- * * 0.0.0.0/0 0.0.0.0/0

Chain DOCKER (1 references)
  pkts bytes target prot opt in out source destination

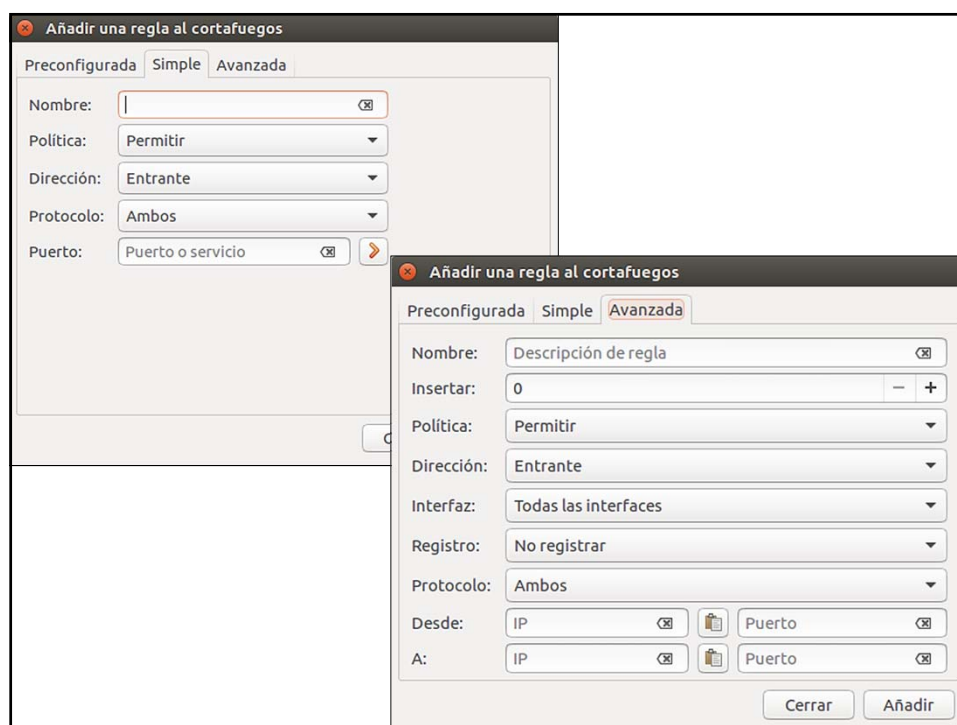
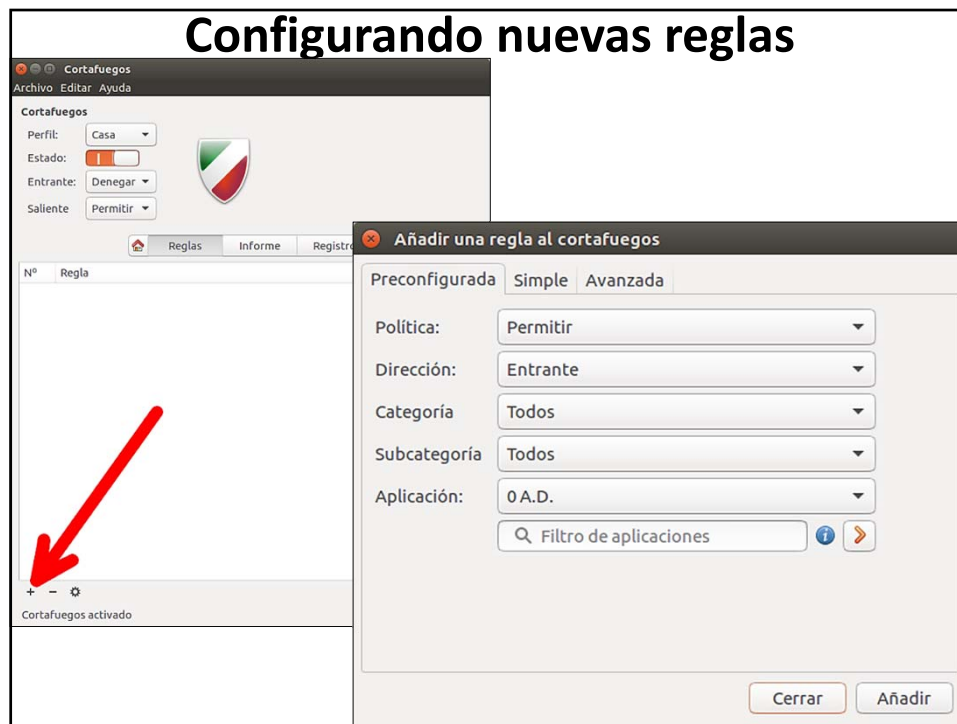
```

Instalación de Gufw en un sistema gráfico: `sudo apt-get install gufw`



Secuencia de gestión de reglas





Para entregar

- Una vez finalizada la práctica deberás entregar:
 - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
 - Las pantallas más significativas que demuestren la ejecución
- Nomenclatura identificativa de práctica:
 - **PARP412-Cortafuegos-ufw**