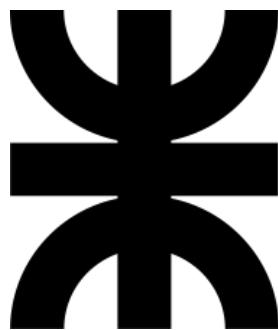


Universidad Tecnológica Nacional

Facultad Regional Córdoba

Ingeniería en Sistemas de Información

Redes de Datos



IMPLEMENTACIÓN DE FIREWALL

Trabajo Práctico Nro. 6

Año: 2025

Curso: 4k1

Grupo Nro: 2

Integrantes:

| | |
|---------------------------------|-------|
| Baigorria, José Alejó | 96269 |
| Buchaillot, Julieta | 95782 |
| Garcia, Florencia Daniela | 94477 |
| Lucini, Gabriel Alejandro | 98023 |
| Martinet, Agustina María Andrea | 94674 |
| Milhas Mac Dougall, Mariana | 95257 |

Índice

| | |
|---|----------|
| Índice..... | 2 |
| Configuraciones..... | 1 |
| Configuración servidor..... | 1 |
| Configuración cliente..... | 3 |
| Configuración firewall..... | 4 |
| Configuración server postgres..... | 5 |
| Configuración server LAMP..... | 6 |
| Configuración server de Servidor de Archivos..... | 7 |
| Configuración de una regla..... | 8 |
| Reglas definidas..... | 9 |

Configuraciones

Configuración servidor

```
Starting Unbound DHCP Leases Bridge... [ OK ]
Starting Apache daemon... [ OK ]
Starting fcron... [ OK ]

IPFire v2.29 - www.ipfire.org
=====
ipfire.localdomain running on Linux 6.12.34-ipfire x86_64
ipfire login: root
Password:
Login incorrect

ipfire.localdomain login:
ipfire.localdomain login: admin
Password:
Login incorrect

ipfire.localdomain login:
Login timed out after 60 seconds.

IPFire v2.29 - www.ipfire.org
=====
ipfire.localdomain running on Linux 6.12.34-ipfire x86_64
ipfire login: root
Password:
No mail.
[root@ipfire ~]#
```

```
green0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.50.1 netmask 255.255.255.0 broadcast 0.0.0.0
        ether 08:00:27:db:0b:b9 txqueuelen 1000 (Ethernet)
        RX packets 767 bytes 167570 (163.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1221 bytes 1109206 (1.0 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        device interrupt 19 base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4077 bytes 224921 (219.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4077 bytes 224921 (219.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

red0: flags=67<UP,BROADCAST,RUNNING> mtu 1500
        inet 192.168.1.21 netmask 255.255.255.0 broadcast 192.168.1.255
        ether 08:00:27:24:89:30 txqueuelen 1000 (Ethernet)
        RX packets 1896 bytes 1224736 (1.1 MiB)
        RX errors 6 dropped 0 overruns 0 frame 0
        TX packets 943 bytes 194324 (189.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        device interrupt 16 base 0xd240
```

El servidor está configurado con un esquema de red típico de IPFire, utilizando las interfaces **red (WAN)** y **green (LAN)**, además de la interfaz de loopback. Las configuraciones observadas son las siguientes:

Interfaz Green (LAN Interna)

- **IP asignada:** 192.168.50.1
- **Máscara de red:** 255.255.255.0
- **Función:** Red interna segura.
- **Descripción:** Esta interfaz actúa como el punto de acceso principal para los dispositivos de la red local. La dirección 192.168.50.1 opera como puerta de enlace para los hosts internos y permite la interacción controlada con redes externas a través del firewall.

Interfaz Red (WAN o Red Externa)

- **IP asignada:** 192.168.1.21
- **Máscara de red:** 255.255.255.0
- **Función:** Conexión hacia la red externa.
- **Descripción:** Esta interfaz representa la conexión del servidor hacia una red externa (por ejemplo, un router superior o el segmento que simula Internet en el laboratorio). A través de ella se gestiona el tráfico entrante y saliente sujeto a las políticas de firewall.

En definitiva, la interfaz *green* se encuentra destinada exclusivamente a la red local confiable, mientras que *red* se utiliza como puerta hacia redes no confiables o externas, manteniendo así un esquema de protección y segmentación característico de entornos firewall.

Configuración cliente

El equipo cliente fue configurado con la red Interna de nombre redGREEN. Al encenderse, obtuvo su configuración de red automáticamente del DHCP del Firewall. El comando ip adres demuestra la asignación exitosa de una dirección IP dentro del rango permitido de la Red GREEN, específicamente 192.168.50.102.

Esta configuración inicial asegura que el tráfico entre el Cliente (GREEN) y los Servidores (RED) deba pasar obligatoriamente por el Firewall, permitiendo la posterior implementación y prueba de las reglas de filtrado.

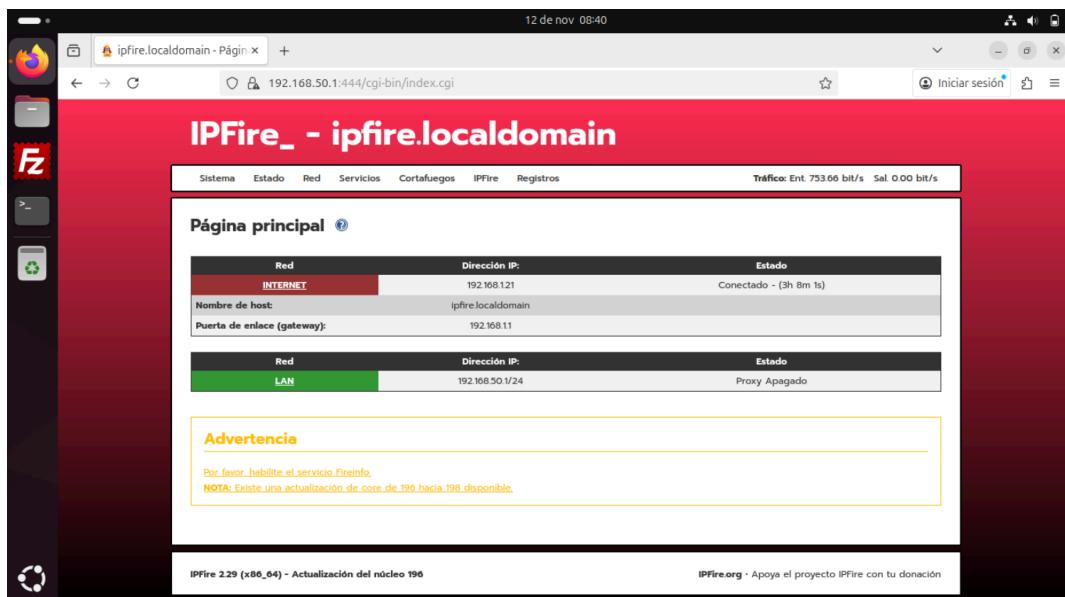
```
usuario@Debian24-cliente:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:bf:fe:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.102/24 brd 192.168.50.255 scope global dynamic noprefixroute
        enp0s3
            valid_lft 2435sec preferred_lft 2435sec
        inet6 fe80::a00:27ff:febff:fe4f/64 scope link
            valid_lft forever preferred_lft forever
```

Configuración firewall

Para confirmar que la configuración inicial de las zonas de red ha sido aplicada correctamente, accedemos a la interfaz de administración web del Firewall (IPFire) desde el cliente. Aquí verificamos el estado del sistema y, más importante, el direccionamiento de las interfaces:

- La zona Red LAN (GREEN) muestra la IP 192.168.50.1/24, confirmando que esta es la puerta de enlace activa para nuestra red de clientes.
- La zona Red INTERNET (RED) está correctamente "Conectado" y muestra la IP 192.168.1.21, validando la conexión con la red de servicios (RED) y la red física.

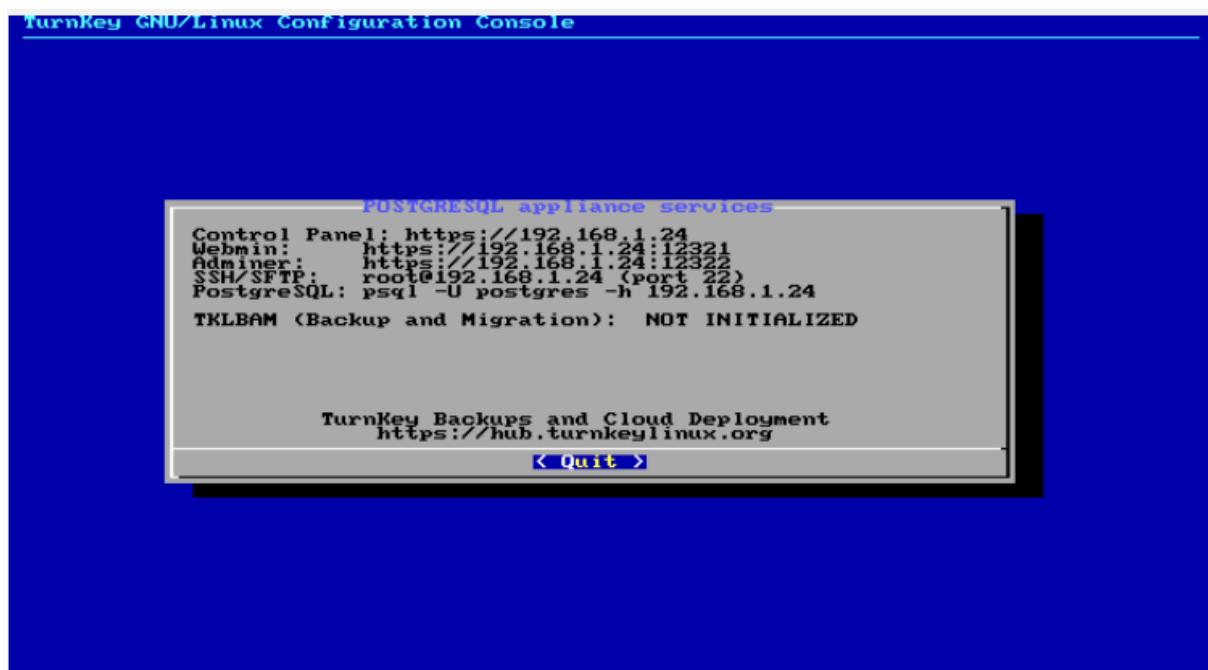
Con esta verificación, dimos por terminado el levantamiento de la infraestructura y procedimos a la configuración de las reglas de filtrado en la sección "Cortafuegos".



Configuración server postgres

Ahora procedemos a levantar el Servidor PostgreSQL en la Red RED (Red de Servicios). Lo configuraremos en el hipervisor para que obtuviera una dirección IP dentro del segmento de la red física.

La imagen muestra el *TurnKey GNU/Linux Configuration Console* del servidor, donde verificamos la información para la implementación de las reglas: constatamos que el servidor tomó la IP 192.168.1.24 y registramos los puertos de los servicios que serían objeto del filtrado, tales como Webmin (12321), SSH/SFTP (Puerto 22), y la conexión directa a la base de datos PostgreSQL (Puerto 5432, implícito en el servicio psql). Esta información nos permite establecer los criterios de Destino (IP y Puerto) que utilizaremos en las Listas de Control de Acceso (ACLs) del firewall.

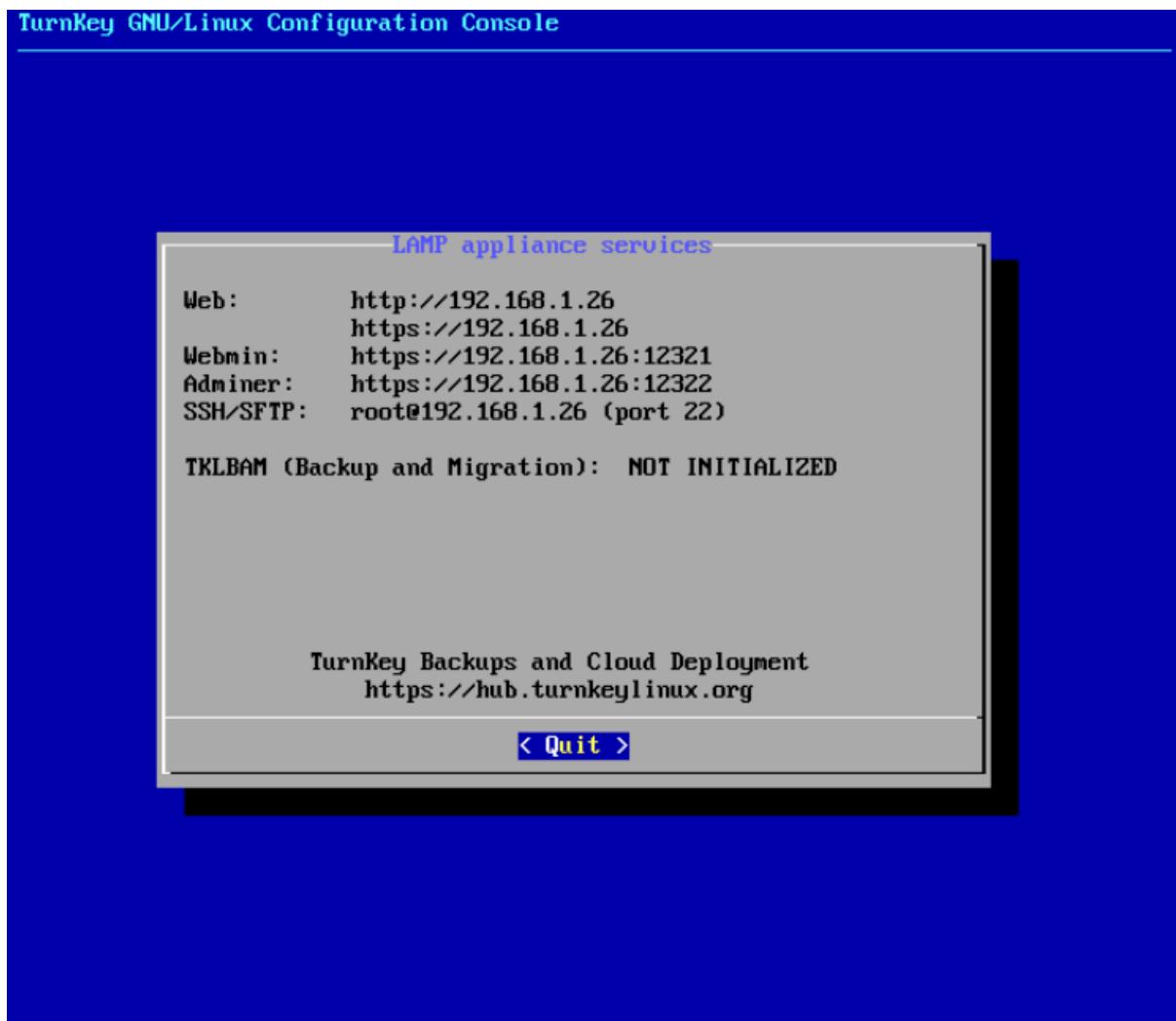


Configuración server LAMP

En la consola de configuración se observa cómo se encuentra configurado el servidor LAMP.

Vemos que el sistema ha sido correctamente desplegado con la dirección IP 192.168.1.26, a través de la cual se encuentran habilitados todos los servicios principales. El mismo se encuentra activo y preparado para atender requerimientos de aplicaciones web con o sin cifrado.

Entre las herramientas administrativas que se incluye, tenemos Webmin, accesible mediante la dirección segura <https://192.168.1.26:12321>, desde donde es posible realizar la gestión del sistema y realizar ajustes de configuración sin necesidad de acceder directamente por consola. Para la administración de bases de datos, el servidor ofrece la herramienta Adminer, disponible en <https://192.168.1.26:12322>. También se encuentra habilitado el acceso por SSH en el puerto 22, permitiendo el ingreso del administrador mediante el usuario root, tanto para tareas de mantenimiento como para transferencias seguras de archivos mediante SFTP.

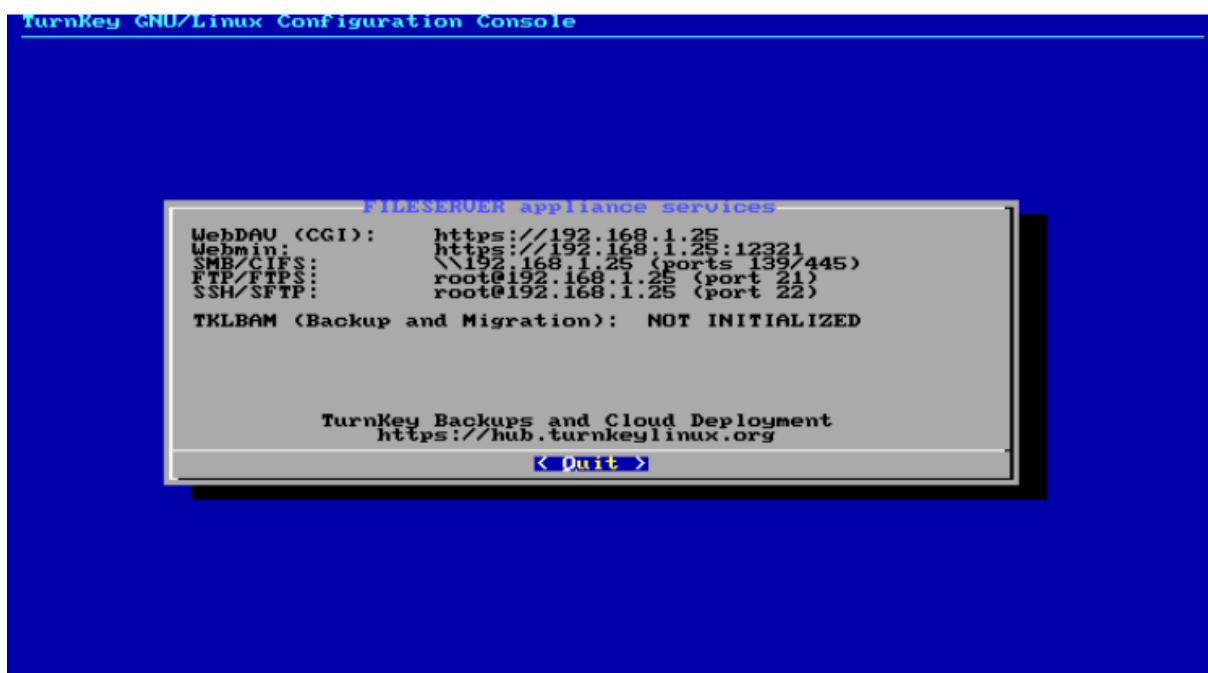


Configuración server de Servidor de Archivos

El servidor **FileServer** de TurnKey Linux, se encuentra configurado con la dirección IP **192.168.1.25**, desde la cual se habilitan los distintos servicios de acceso y administración. El servidor ofrece múltiples protocolos para compartir y administrar archivos: WebDAV mediante HTTPS, accesible desde navegadores y clientes compatibles; SMB/CIFS en los puertos 139 y 445, y FTP/FTPS a través del puerto 21, tanto para transferencias normales como cifradas.

Además, el servidor habilita acceso administrativo mediante Webmin en el puerto seguro **12321**, permitiendo la configuración completa del sistema desde una interfaz web. También se encuentra disponible el acceso por **SSH y SFTP** en el puerto 22 mediante el usuario root, facilitando la administración avanzada y la transferencia segura de archivos.

Todos estos servicios funcionan sobre la misma dirección IP, por lo que el acceso se realiza simplemente indicando el protocolo correspondiente.



Configuración de una regla

Para demostrar la configuración de una regla, elegimos aquella que tiene el objetivo de permitir el acceso al servicio Webmin (12321) del Servidor LAMP desde nuestra red interna (GREEN).

La imagen muestra el formulario de Reglas del Cortafuegos con los parámetros establecidos:

1. Origen (Source): Definimos la red de origen como 192.168.50.0/24 (la Red GREEN). Esto asegura que la regla solo aplique al tráfico proveniente de nuestros clientes internos.
2. Destino (Destination): Especificamos la dirección IPv4 del Servidor LAMP, que es 192.168.1.26.
3. Protocolo: Seleccionamos TCP y establecemos el Puerto de Destino como 12321, que corresponde al servicio Webmin del Servidor LAMP.
4. Acción: Finalmente, elegimos la acción **ACEPTAR** para permitir el tráfico que coincida con todos los criterios anteriores.

Reglas del Cortafuegos ⓘ

Origen

Dirección de origen (dirección MAC/IP o red):
 Redes estándar:
 Ubicación

Firewall

NAT

Usar traducción de direcciones de red (NAT)

Destino

Dirección de destino (dirección IP o red):
 Redes estándar:
 Ubicación

Firewall

Protocolo

Puerto de origen:
Puerto de destino:

ACEPTAR DESCARTAR RECHAZAR

Ajustes adicionales

Observación:
Posición de la

Reglas definidas

Después de desactivar la regla general de permiso del firewall (que permite todo el tráfico de GREEN a RED), procedimos a implementar las 15 reglas de filtrado solicitadas por el docente. Estas reglas se configuraron como ACLs (Listas de Control de Acceso) en la interfaz web de IPFire, controlando el tráfico basado en la red de Origen, la IP de Destino, el Protocolo, y el Puerto.

Para las reglas que involucraban servicios no montados, utilizamos el direccionamiento virtual asignado:

- Servidor Web (Regla 12): 192.168.1.27
- Servidor NTP (Regla 13): 192.168.1.28
- Servidor Telnet (Regla 14): 192.168.1.29
- Servidor Mail (Regla 15): 192.168.1.30

Para las reglas que requieren la IP de un cliente GREEN (Reglas 3, 9, 10, 11, 12, 13 y 15), utilizamos la dirección 192.168.50.102.

Con todas las reglas implementadas, procedimos a la fase de verificación y pruebas para comprobar que tanto los accesos permitidos como los rechazos funcionaran correctamente.

| Regla | Origen | Destino | Condición | Servicio/Protocolo |
|----------|------------------------|----------------------|-----------|--------------------|
| Regla 1 | Red GREEN entera | Servidor LAMP | Permitir | Web adminer |
| Regla 2 | Red GREEN entera | Servidor LAMP | Permitir | SSH |
| Regla 3 | IP de un cliente GREEN | Servidor LAMP | Rechazar | ICMP |
| Regla 4 | Red GREEN entera | Servidor de archivos | Permitir | SMB/CIFS |
| Regla 5 | Red GREEN entera | Servidor de archivos | Permitir | FTP |
| Regla 6 | Red GREEN entera | Servidor de archivos | Permitir | SSH |
| Regla 7 | Red GREEN entera | Servidor de archivos | Rechazar | ICMP |
| Regla 8 | Red GREEN entera | Servidor Postgres | Rechazar | Web adminer |
| Regla 9 | IP de un cliente GREEN | Servidor Postgres | Permitir | BD Postgres |
| Regla 10 | IP de un cliente GREEN | Servidor Postgres | Permitir | SSH |
| Regla 11 | IP de un cliente GREEN | Servidor Postgres | Rechazar | ICMP |
| Regla 12 | IP de un cliente GREEN | Servidor Web | Permitir | HTTPS |
| Regla 13 | IP de un cliente GREEN | Servidor NTP | Rechazar | NTP |
| Regla 14 | Red GREEN entera | Servidor Telnet | Rechazar | Telnet |
| Regla 15 | IP de un cliente GREEN | Servidor Mail | Rechazar | POP3 |

Reglas del Cortafuegos

| # | Protocolo | Origen | Registro | Destino | Acción |
|----------|-----------|----------------|--------------------------|----------------------|-------------------------------------|
| 1 | TCP | Green | <input type="checkbox"/> | 192.168.1.26: 12322 | <input checked="" type="checkbox"/> |
| 2 | TCP | Green | <input type="checkbox"/> | 192.168.1.26: 22 | <input checked="" type="checkbox"/> |
| 3 | ICMP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.26 | <input checked="" type="checkbox"/> |
| 4 | TCP | Green | <input type="checkbox"/> | 192.168.1.25: 139 | <input checked="" type="checkbox"/> |
| 5 | TCP | Green | <input type="checkbox"/> | 192.168.1.25: 445 | <input checked="" type="checkbox"/> |
| 6 | TCP | Green | <input type="checkbox"/> | 192.168.1.25: 21 | <input checked="" type="checkbox"/> |
| 7 | TCP | Green | <input type="checkbox"/> | 192.168.1.25: 22 | <input checked="" type="checkbox"/> |
| 8 | ICMP | Green | <input type="checkbox"/> | 192.168.1.25 | <input checked="" type="checkbox"/> |
| 9 | TCP | Green | <input type="checkbox"/> | 192.168.1.24: 12322 | <input checked="" type="checkbox"/> |
| 10 | TCP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.24: 5432 | <input checked="" type="checkbox"/> |
| 11 | TCP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.24: 22 | <input checked="" type="checkbox"/> |
| 12 | ICMP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.24 | <input checked="" type="checkbox"/> |
| 13 | TCP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.27: HTTPS | <input checked="" type="checkbox"/> |
| 14 | UDP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.28: NTP | <input checked="" type="checkbox"/> |
| 15 | TCP | Green | <input type="checkbox"/> | 192.168.1.29: Telnet | <input checked="" type="checkbox"/> |
| 16 | TCP | 192.168.50.102 | <input type="checkbox"/> | 192.168.1.30: POP3 | <input checked="" type="checkbox"/> |
| Regla 15 | | | | | |

Aclaración: SMB/CIFS usa dos puertos (139 y 445). Como el firewall trabaja por puerto, para permitir el acceso al servidor de archivos desde la red GREEN fue necesario crear dos reglas, una por cada puerto. A partir de la regla 5, los números quedan desfasados con respecto a la tabla.