



ACTIVIDAD INTEGRADORA VI

IMPLEMENTACIÓN DE FIREWALL

**Carrera:** Ingeniería en sistemas de Información

**Asignatura:** Redes de Datos

**Curso:** 4K1

**Docentes:**

- Ing. Fabian Gibellini
- Ing. Leonardo Ciceri

**Integrantes:**

- Delgado Alexis Ezequiel (95227)
- Angonese Juan Pablo (98230)
- Brito Serena (84066)
- Cufre Angel (94490)
- Scrosati Emanuel (95632)

**Grupo Nro:** 17

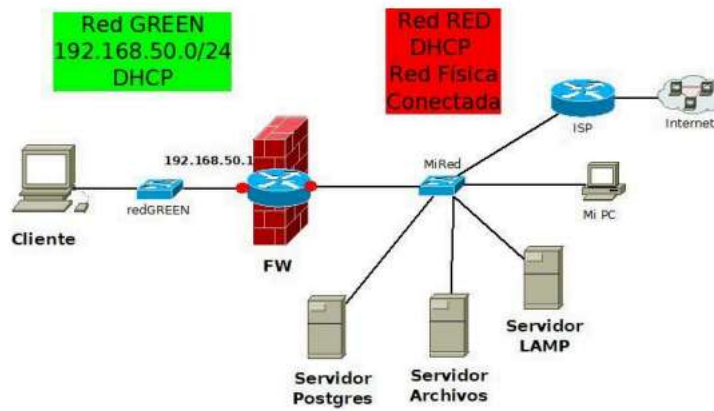
## Índice

|  |    |
|--|----|
| OBJETIVOS                                  | 2  |
| Topología                                  | 2  |
| Máquina Virtual IPFire_FW                  | 2  |
| Levantar servidores                        | 4  |
| Servidor de archivos                       | 4  |
| Servidor postgresql                        | 4  |
| Servidor LAMP                              | 5  |
| Prueba de servidores                       | 5  |
| Servidor de archivos, Web adminer:         | 5  |
| Servidor Postgresql, Servicio BD Postgres: | 6  |
| Servidor LAMP, Web adminer:                | 6  |
| Configuración del Firewall                 | 7  |
| Regla 1                                    | 7  |
| Regla 2                                    | 9  |
| Regla 3                                    | 10 |
| Regla 4                                    | 12 |
| Regla 5                                    | 14 |
| Regla 6                                    | 16 |
| Regla 7                                    | 18 |
| Regla 8                                    | 20 |
| Regla 9                                    | 21 |
| Regla 10                                   | 23 |
| Regla 11                                   | 25 |
| Regla 12                                   | 26 |
| Regla 13                                   | 26 |
| Regla 14                                   | 27 |
| Regla 15                                   | 27 |
| Reglas configuradas                        | 28 |

## OBJETIVOS:

- Analizar el propósito y la aplicación de ACLs en la gestión del tráfico de red.
- Implementar las reglas de filtrado definidas por el docente en una herramienta software.
- Definir y probar reglas para permitir o denegar tráfico según criterios específicos (IP de origen/destino, puertos, protocolos).
- Verificar y depurar la configuración de firewall al utilizar comandos y pruebas (ping, traceroute, logs) para confirmar el correcto funcionamiento de la ACL aplicada.

## Topología



## Máquina Virtual IPFire\_FW

Luego de importar la máquina virtual y configurar el networking de las tarjetas de red en zona RED y GREEN. La interfaz green0 debe tomar la IP fija "192.160.50.1", mientras que la interfaz red0 obtendrá una IP automáticamente desde la red física a la que esté conectada la máquina anfitriona.

Para verificar la asignación de IPs, se ejecuta el siguiente comando en consola (ifconfig):

```
Bye bye.

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 ~]# ifconfig
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:f9:1f:23 txqueuelen 1000 (Ethernet)
    RX packets 18648 bytes 4377535 (4.1 MiB)
    RX errors 1 dropped 0 overruns 0 frame 0
    TX packets 26351 bytes 14165476 (13.5 MiB)
    TX errors 0 dropped 4 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0xd020

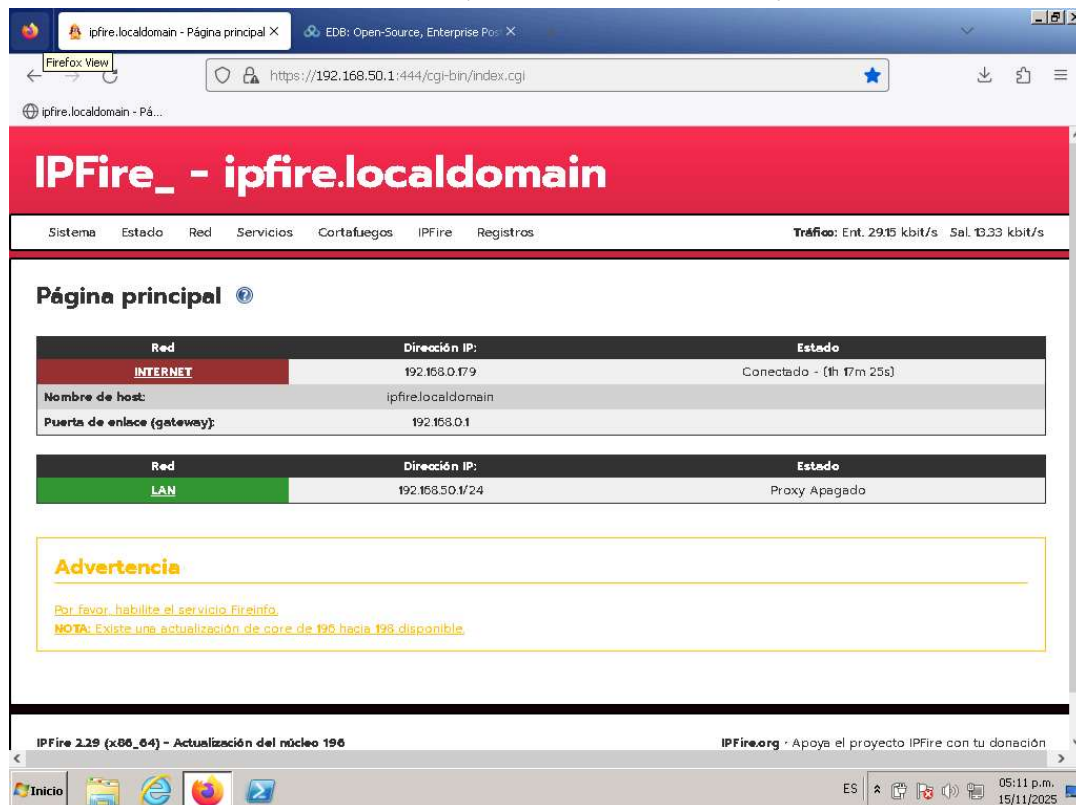
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12115 bytes 698594 (682.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12115 bytes 698594 (682.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

red0: flags=67<UP,BROADCAST,RUNNING> mtu 1500
    inet 192.168.0.179 netmask 255.255.255.0 broadcast 192.168.0.255
    ether 08:00:27:32:a0:69 txqueuelen 1000 (Ethernet)
    RX packets 6045 bytes 2288041 (2.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3104 bytes 362581 (354.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ipfire ~]# Delgado Alexis, Angonese Juan Pablo, Cufre Angel, Brito Serena, Scrosati Emanuel_
```

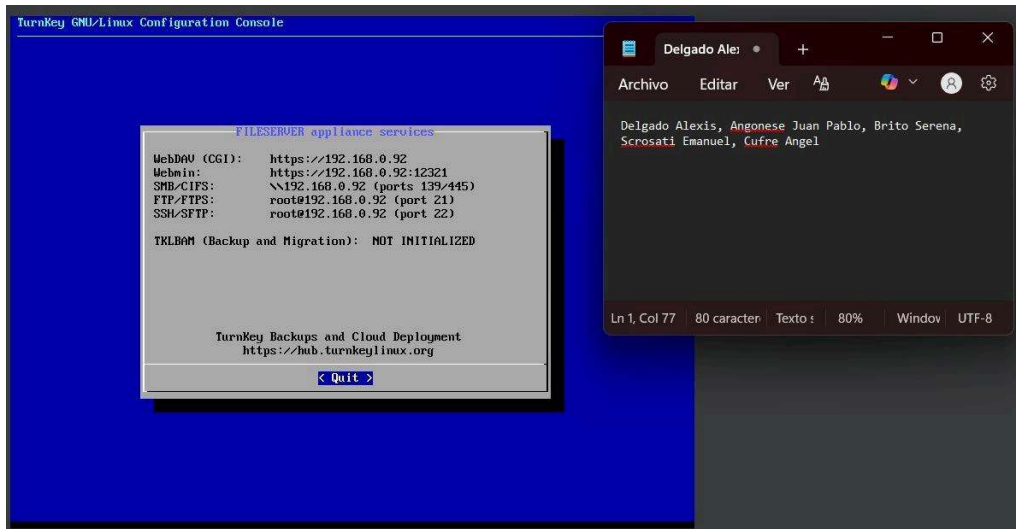
En este caso corroboramos que la ip asignada a la red green es “192.168.50.1” y a la red0 se le asigno la “192.168.0.179”

Accediendo a la interfaz web del FW (<https://192.168.50.1:444/>) tambien lo corroboramos:

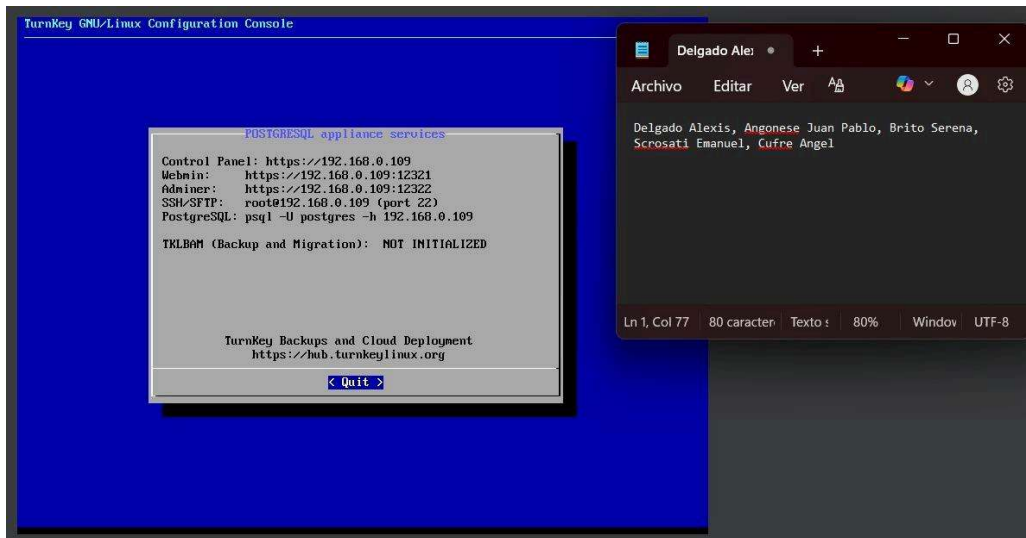


## Levantar servidores:

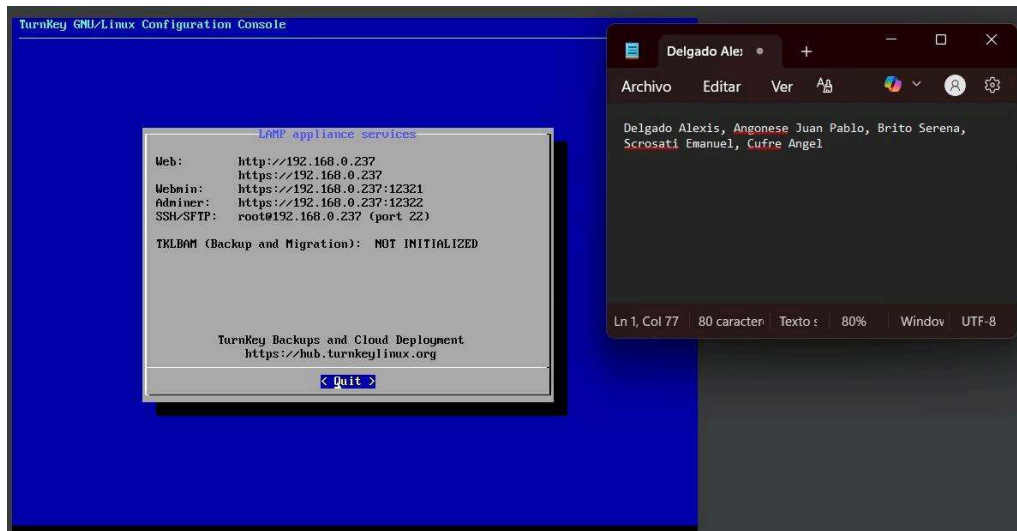
### Servidor de archivos



### Servidor postgresql



## Servidor LAMP

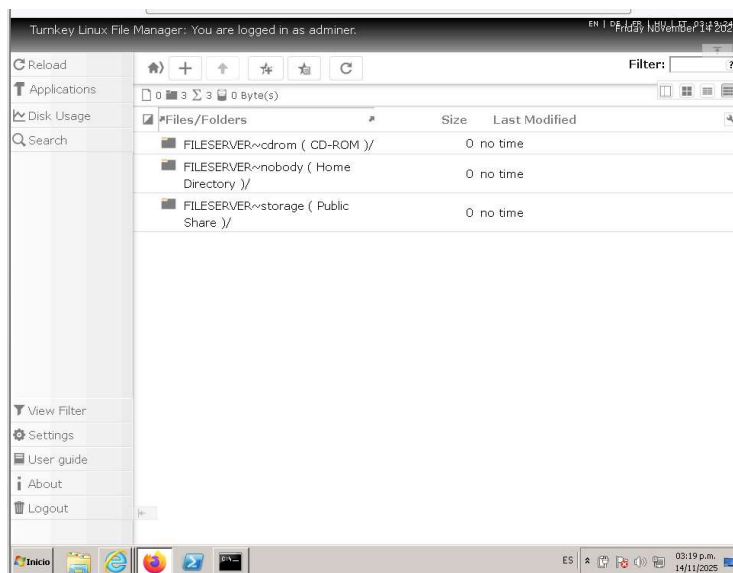


## Prueba de servidores:

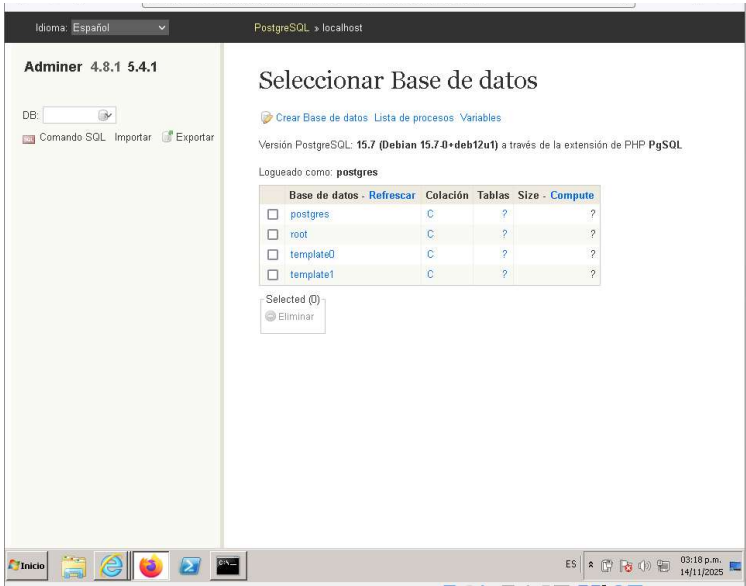
Antes de aplicar las reglas en el firewall, verificamos que los servicios estén activos en los servidores.

Como todavía no hemos configurado ninguna regla restrictiva, los equipos de la red green deberían tener acceso a la red RED, por lo que los servidores deberían estar levantados y accesibles. Esta conectividad nos permite validar que hemos configurado correctamente la red. Se muestran algunos ejemplos:

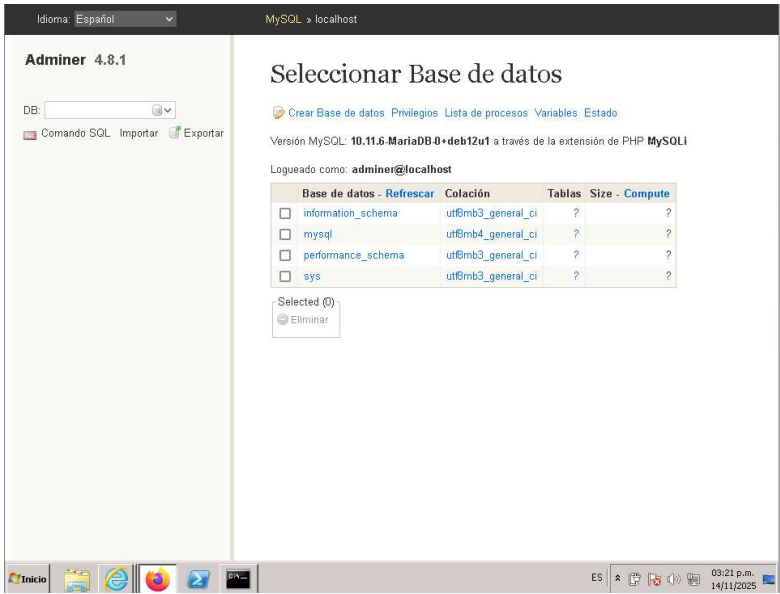
## Servidor de archivos, Web adminer:



Servidor Postgresql, Servicio BD Postgres:



Servidor LAMP, Web adminer:



## Configuración del Firewall

Listado de reglas de firewall a aplicar:

| Grupo 17 |                        |                       |           |                    |
|----------|------------------------|-----------------------|-----------|--------------------|
| Regla    | Origen                 | Destino               | Condicion | Servicio/Protocolo |
| Regla 1  | IP de un cliente GREEN | Servidor LAMP         | Rechazar  | Web adminer        |
| Regla 2  | Red GREEN entera       | Servidor LAMP         | Rechazar  | SSH                |
| Regla 3  | IP de un cliente GREEN | Servidor LAMP         | Permitir  | ICMP               |
| Regla 4  | Red GREEN entera       | Servidor de archivos  | Permitir  | SMB/CIFS           |
| Regla 5  | Red GREEN entera       | Servidor de archivos  | Permitir  | FTP                |
| Regla 6  | IP de un cliente GREEN | 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  | Red GREEN entera       | Servidor Postgres     | Rechazar  | BD Postgres        |
| Regla 10 | IP de un cliente GREEN | Servidor Postgres     | Rechazar  | SSH                |
| Regla 11 | IP de un cliente GREEN | Servidor Postgres     | Permitir  | ICMP               |
| Regla 12 | IP de un cliente GREEN | Servidor Telnet       | Permitir  | Telnet             |
| Regla 13 | Red GREEN entera       | Servidor BD SqlServer | Rechazar  | BD SqlServer       |
| Regla 14 | Red GREEN entera       | Servidor NTP          | Permitir  | NTP                |
| Regla 15 | Red GREEN entera       | Servidor BD Mysql     | Permitir  | BD Mysql           |

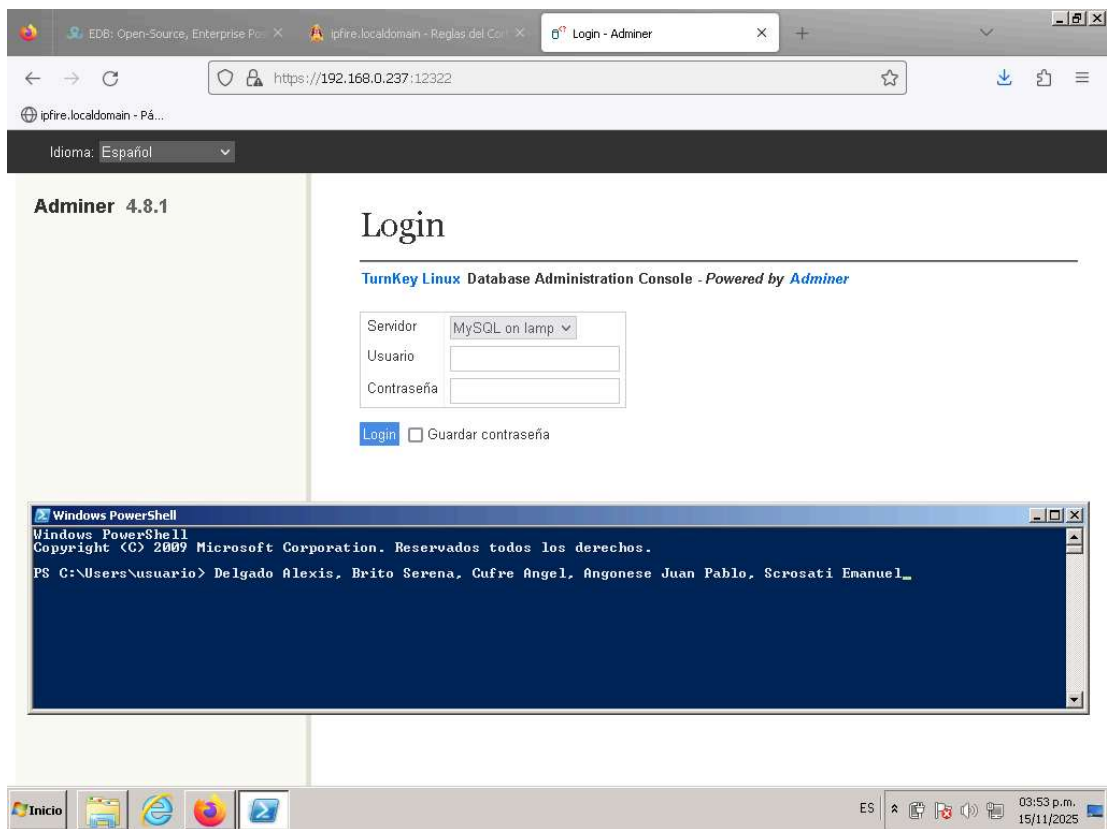
### Regla 1

| Origen                 | Destino       | Condición | Servicio/Protocolo |
|------------------------|---------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor LAMP | Rechazar  | Web adminer        |

Esta regla tiene como objetivo bloquear el acceso a la interfaz de administración web (Web adminer) desde una IP específica de la red GREEN en este caso 192.168.50.101.

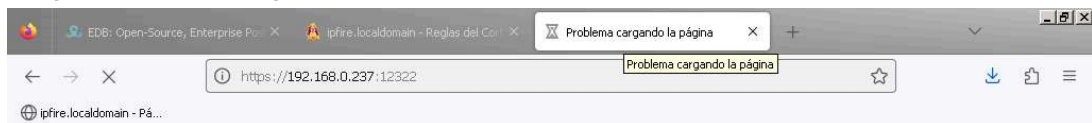
Antes de aplicar la regla accedemos a la interfaz de administración web Adminer mediante el navegador, utilizando la dirección <https://192.168.0.237:12322/> :





Corroboramos el ingreso exitoso.

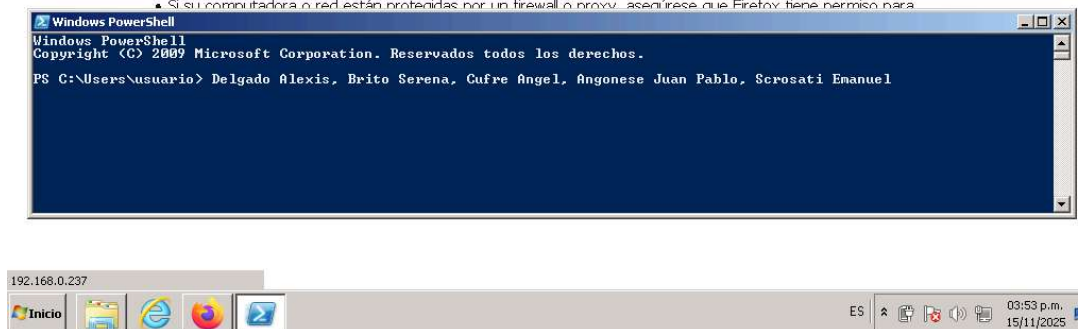
Luego de aplicar la regla:



## La conexión tardó demasiado tiempo

Ocurrió un error al conectarse a 192.168.0.237:12322.

- El sitio puede no estar disponible temporalmente o estar sobrecargado. Intente nuevamente en unos momentos.
- Si no puede cargar ninguna página, verifique la conexión de su computadora a la red.
- Si su computadora o red están protegidas por un firewall o proxy, asegúrese que Firefox tiene permiso para



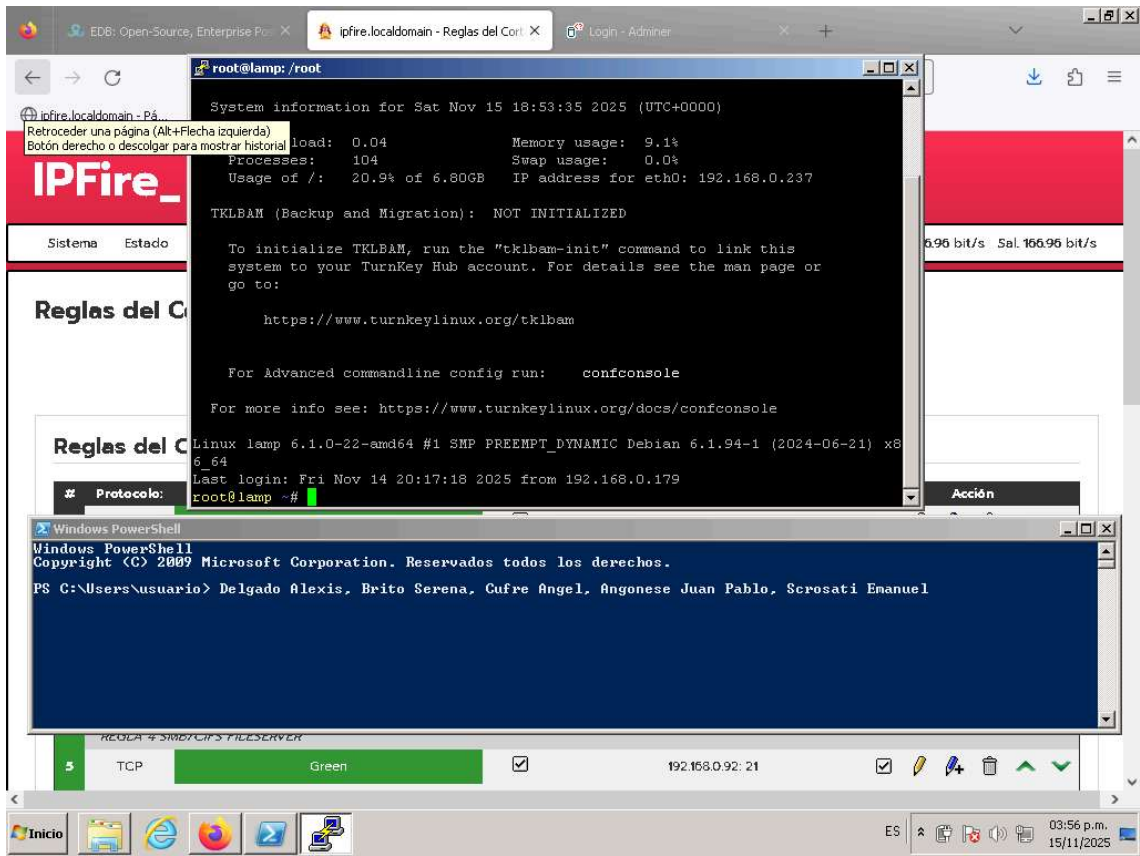
La conexión falla al intentar acceder al servicio en el puerto correspondiente, lo que indica que la regla aplicada en el firewall está funcionando correctamente. Este comportamiento confirma que el tráfico ha sido filtrado según lo establecido, impidiendo el acceso desde la red GREEN al servicio especificado.

Regla 2

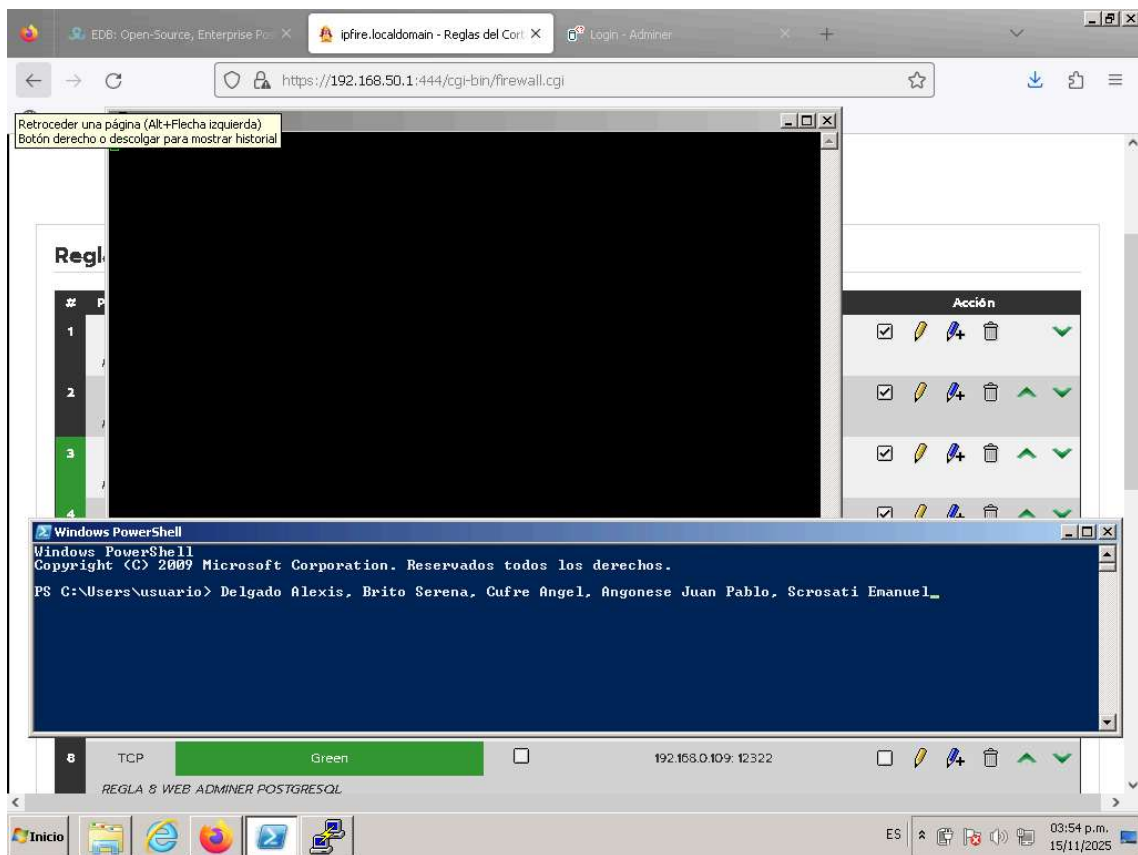
| Origen           | Destino       | Condición | Servicio/Protocolo |
|------------------|---------------|-----------|--------------------|
| Red GREEN entera | Servidor LAMP | Rechazar  | SSH                |

Esta regla tiene como objetivo bloquear el acceso remoto por SSH (puerto 22), desde cualquier equipo de la red GREEN hacia el servidor LAMP.

Para corroborar el funcionamiento de la regla ingresamos a “PuTTY ” ingresando la ip 192.168.0.237 y puerto 22 antes de aplicar la regla:



Nos permite establecer la conexión. Luego de aplicar la regla:



La conexión falla y PuTTY muestra el siguiente mensaje de error:  
 “Network error: Connection timed out”, no se pudo establecer comunicación con el servidor tal como lo establecimos en la regla.

### Regla 3

| Origen                 | Destino       | Condición | Servicio/Protocolo |
|------------------------|---------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor LAMP | Permitir  | ICMP               |

Esta regla tiene como objetivo permitir que una IP específica de la red GREEN pueda hacer ping(protocolo ICMP) al servidor LAMP, en este caso el IP cliente es “192.168.50.101”.

En este caso, antes de aplicar la regla, aplicamos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma.

Esto consiste en que, por defecto, se bloquea todo el tráfico y solo se permite lo que está definido en las reglas de tipo "Aceptar".

Antes de aplicar la regla, el firewall no permitirá el acceso desde la IP específica de la red GREEN al servidor LAMP mediante el protocolo ICMP, como se ve en la captura que se muestra a continuación:

```
PS C:\Users\usuario> ping 192.168.0.237
Haciendo ping a 192.168.0.237 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 192.168.0.237:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos).
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel
```

Al realizar una prueba de conectividad (ping) desde una IP de cliente en la red GREEN 192.168.50.101 vemos que la conexión no puede establecerse, ya después de ejecutar el comando nos muestra el mensaje: “Tiempo de espera agotado para la solicitud”

Luego de aplicar la regla:

Volvemos a realizar prueba de conectividad (ping) desde una IP de cliente en la red GREEN 192.168.50.101, en este caso como aplicamos la regla “permitir” se puede establecer la conexión ejecutando el comando ping:

```
Windows PowerShell
PS C:\Users\usuario> ping 192.168.0.237

Haciendo ping a 192.168.0.237 con 32 bytes de datos:
Respuesta desde 192.168.0.237: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.0.237: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.0.237: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.0.237: bytes=32 tiempo=2ms TTL=63

Estadísticas de ping para 192.168.0.237:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms
PS C:\Users\usuario> Delgado Alexis, Cufre Angel, Angonese Juan Pablo, Enmanuel Scrosati, Brito Serena
```

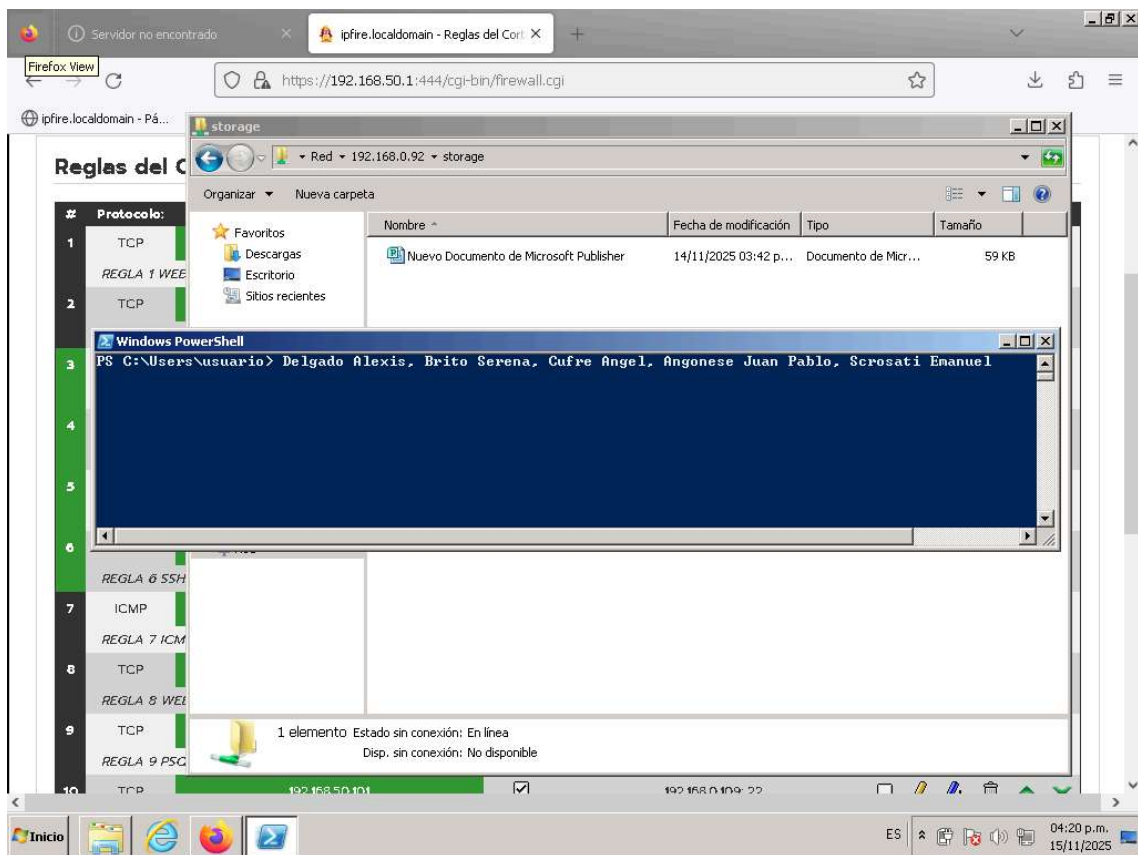
*\*\*nota: en todas las reglas del tipo “permitir” aplicaremos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma.*

Regla 4

| Origen           | Destino              | Condición | Servicio/Protocolo |
|------------------|----------------------|-----------|--------------------|
| Red GREEN entera | Servidor de archivos | Permitir  | SMB/CIFS           |

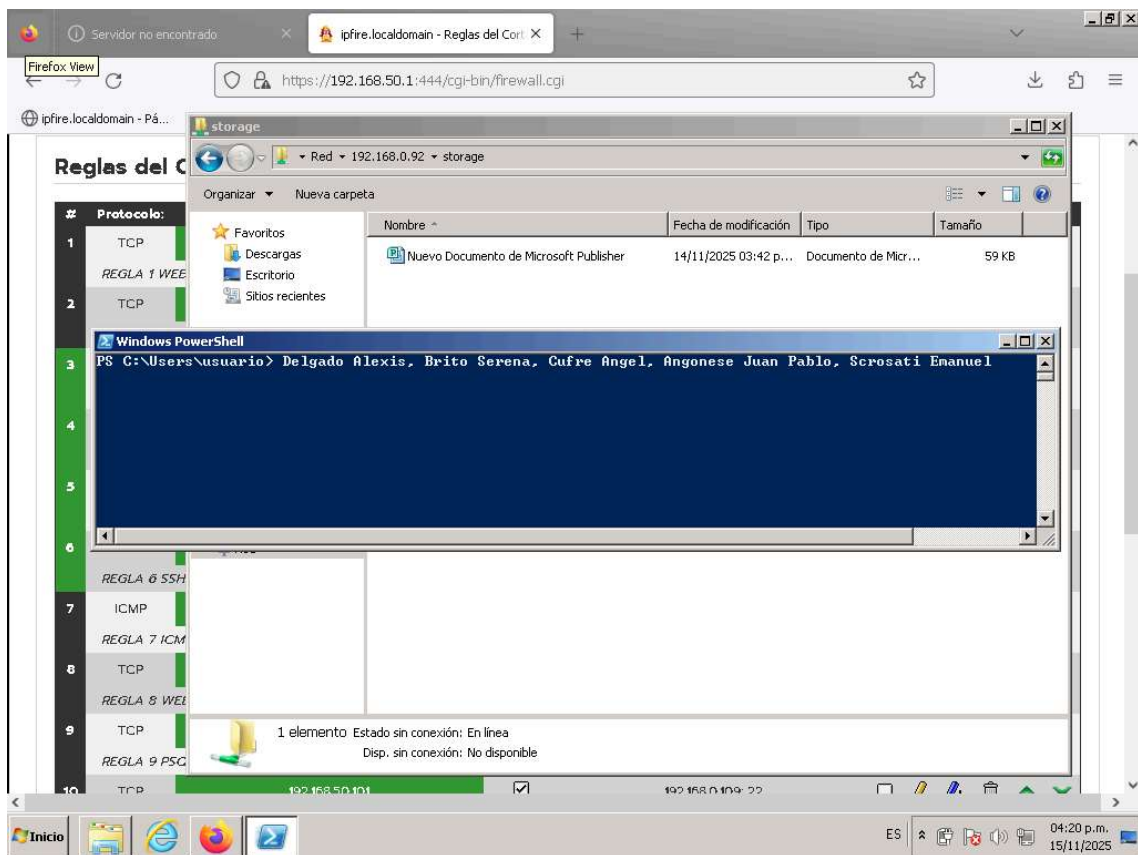
Esta regla tiene como objetivo permitir el acceso SMB/CIFS desde cualquier equipo de la red GREEN a recursos compartidos del servidor de archivos mediante el protocolo SMB/CIFS.

En este caso, antes de aplicar la regla, aplicamos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma. Por lo que, antes de aplicar la regla, el firewall no permitirá el acceso desde la red GREEN al servidor de archivos mediante el protocolo SMB/CIFS, como se ve en la captura:



Luego de aplicar la regla:

Volvemos a acceder al servidor ingresando la dirección \\192.168.0.92 en el explorador de archivos de Windows.



Se logra visualizar correctamente las carpetas compartidas, lo que confirma que el protocolo SMB/CIFS está habilitado

*\*se adjunta video*

## Regla 5

| Origen           | Destino              | Condición | Servicio/Protocolo |
|------------------|----------------------|-----------|--------------------|
| Red GREEN entera | Servidor de archivos | Permitir  | FTP                |

Esta regla tiene como objetivo permitir que cualquier equipo de la red GREEN se conecte al servidor de archivos mediante FTP

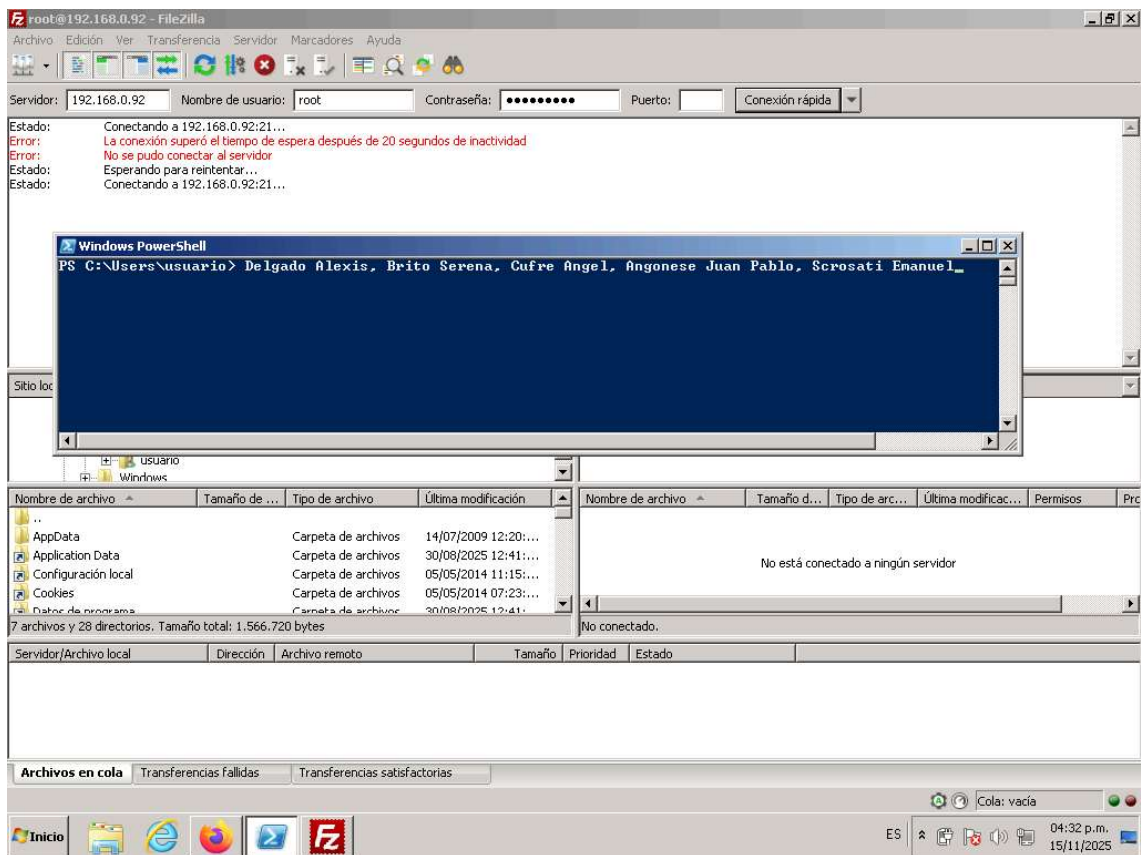
En este caso, antes de aplicar la regla, aplicamos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma.

Antes de aplicar la regla, el firewall no permitirá que se conecte al servidor de archivos mediante FTP desde la red GREEN, para corroborar se utilizó el cliente FileZilla desde una máquina en la red GREEN.

Se configuró la conexión con los siguientes parámetros:

- Servidor: 192.168.0.92
- Usuario: root





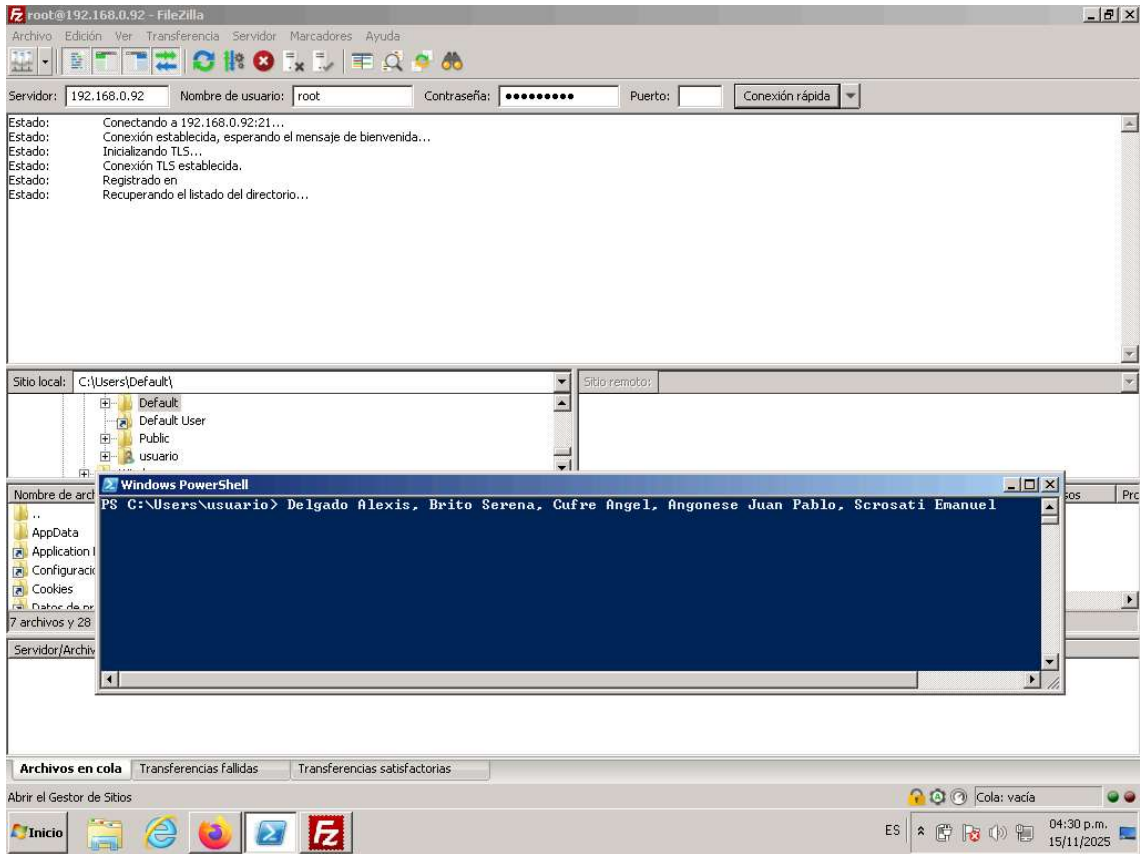
Al iniciar la conexión se observa:

- La conexión superó el tiempo de espera después de 20 segundos de inactividad
- No se pudo conectar al servidor

Esto confirma que el tráfico FTP fue NO permitido por el firewall tal como lo queremos.



Luego de aplicar la regla:Volvemos a utilizar el cliente FileZilla desde una máquina en la red GREEN, configurando los mismo parámetros:



Al iniciar la conexión se observa:

- Conexión establecida
- Inicialización de TLS
- Autenticación exitosa
- Listado de directorios recuperado correctamente

Esto confirma que el tráfico FTP fue permitido por el firewall, y que el servidor respondió correctamente.

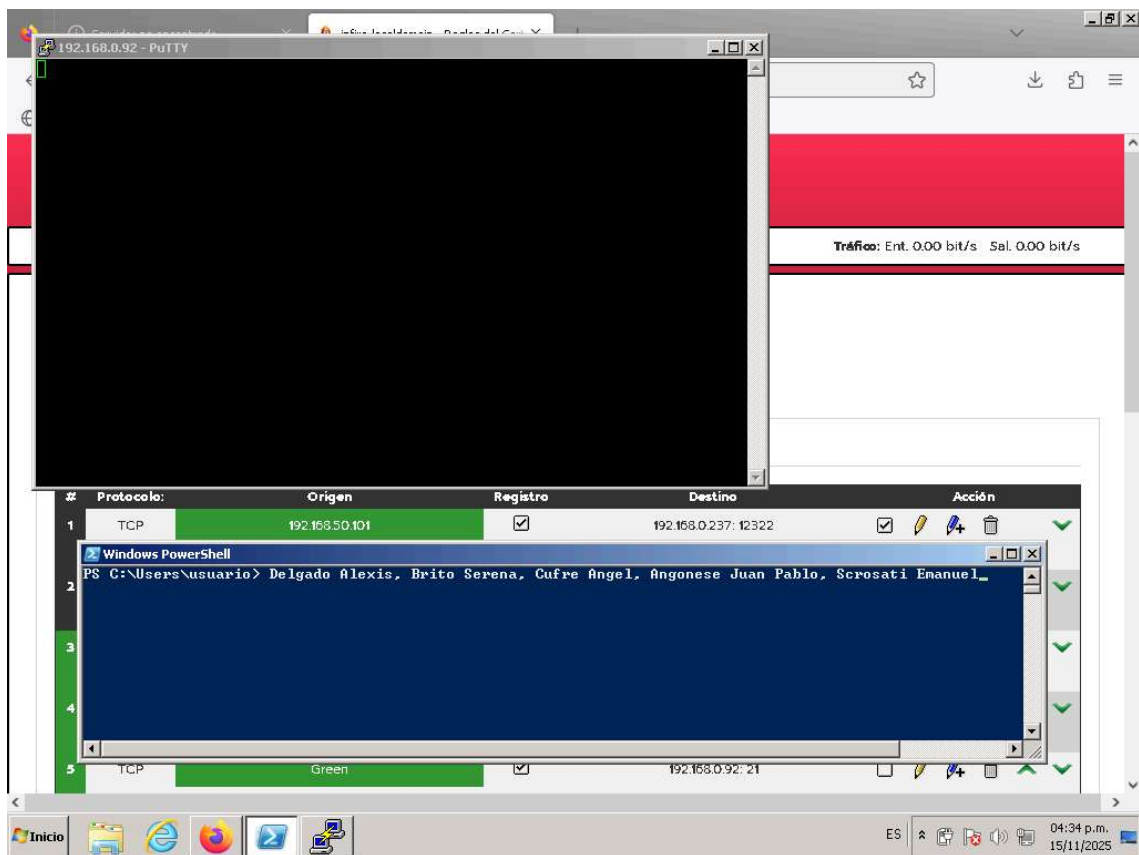
### Regla 6

| Origen                 | Destino              | Condición | Servicio/Protocolo |
|------------------------|----------------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor de archivos | Permitir  | SSH                |

Esta regla tiene como objetivo que una máquina cliente específica en la red GREEN pueda acceder al servidor de archivos por SSH(puerto 22) .

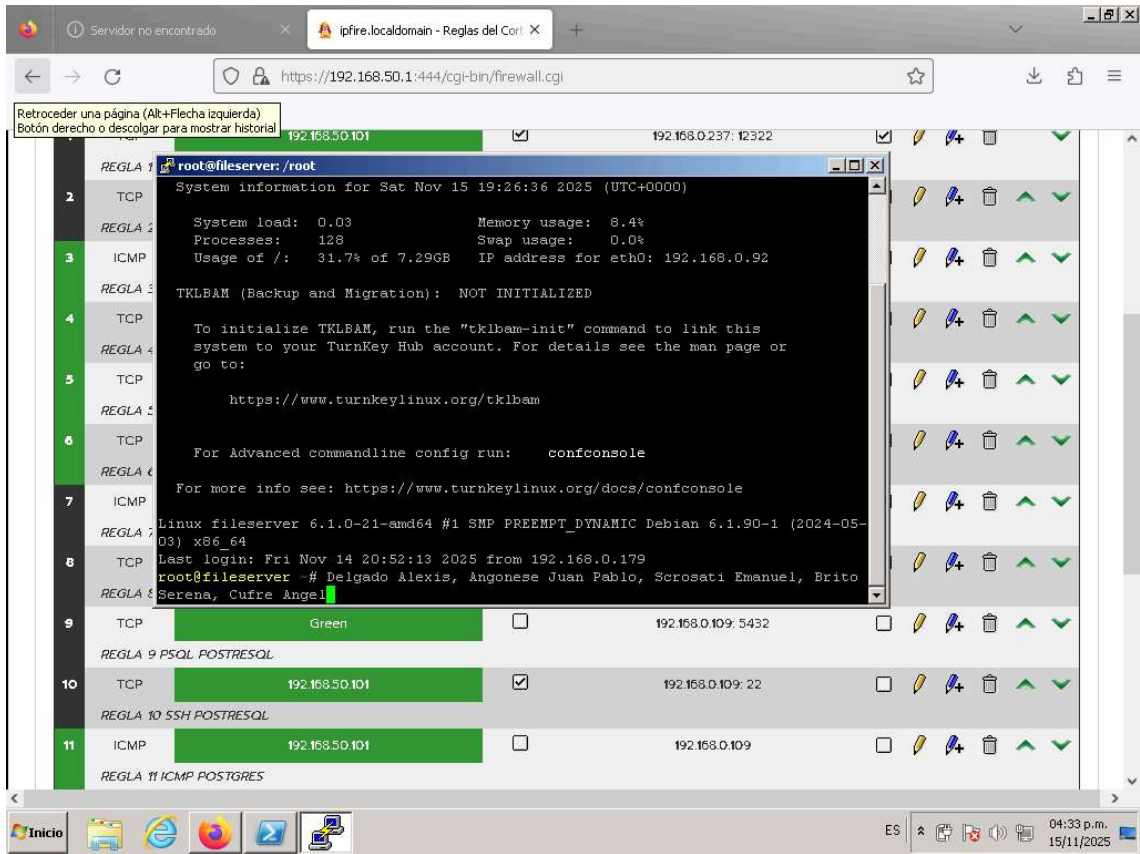
En este caso, antes de aplicar la regla, aplicamos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma.

Ingresamos a "PuTTY " ingresando la ip 192.168.0.92 y puerto 22:



La conexión falla y PuTTY muestra el siguiente mensaje de error:  
"Network error: Connection timed out", no se pudo establecer comunicación con el servidor.  
Luego de aplicar la regla:

Para corroborar el funcionamiento de la regla volvemos a ingresar a “PuTTY ” ingresando la ip 192.168.0.92 y puerto 22:



Se muestra una sesión activa con el prompt de Linux, lo que indica que la conexión fue exitosa.

Regla 7

| Origen           | Destino              | Condición | Servicio/Protocolo |
|------------------|----------------------|-----------|--------------------|
| Red GREEN entera | Servidor de archivos | Rechazar  | ICMP               |

Esta regla tiene como objetivo rechazar ICMP/bloquear el tráfico ICMP desde toda la red GREEN al servidor de archivos.

Se realiza una prueba de conectividad (ping) desde una IP de cliente en la red GREEN al IP 192.168.0.92 antes de aplicar la regla:

```
Windows PowerShell
PS C:\Users\usuario> ping 192.168.0.92

Haciendo ping a 192.168.0.92 con 32 bytes de datos:
Respuesta desde 192.168.0.92: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.0.92: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.0.92: bytes=32 tiempo=5ms TTL=63
Respuesta desde 192.168.0.92: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 192.168.0.92:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 5ms, Media = 2ms
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel
```

Luego de aplicar la regla:

```
Windows PowerShell
PS C:\Users\usuario> ping 192.168.0.92

Haciendo ping a 192.168.0.92 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.92:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
            (100% perdidos),
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel
```

El intento de conexión falla, lo que indica que el tráfico ICMP ha sido correctamente bloqueado por la regla aplicada en el firewall.

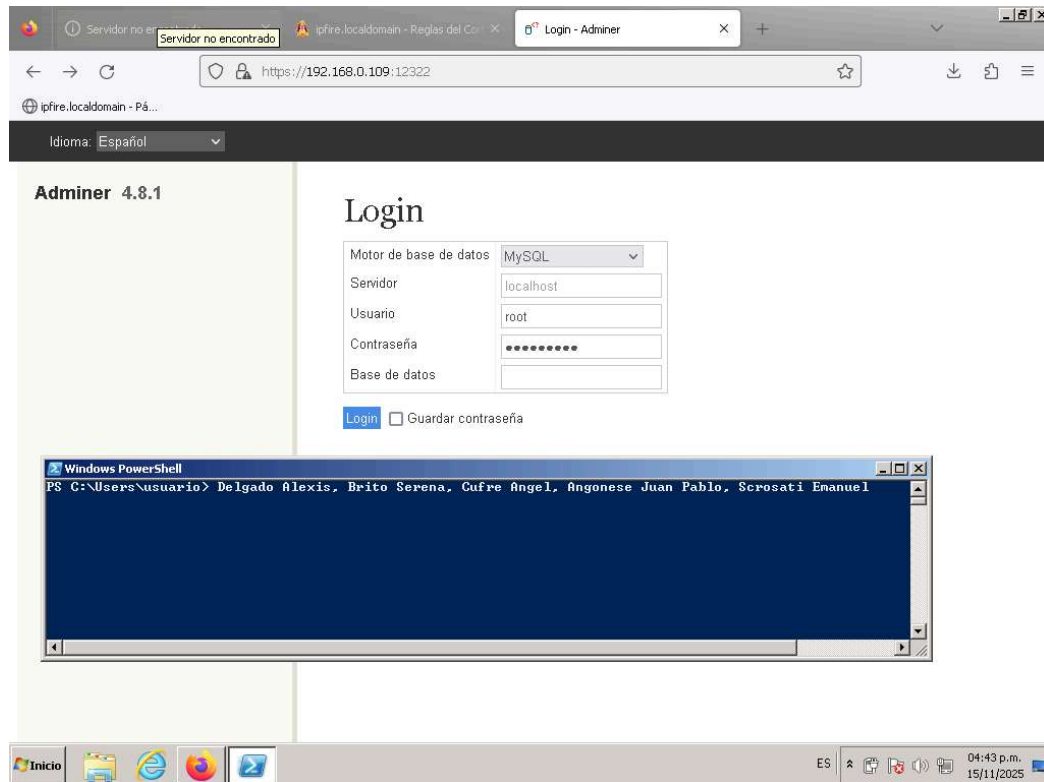
## Regla 8

| Origen           | Destino           | Condición | Servicio/Protocolo |
|------------------|-------------------|-----------|--------------------|
| Red GREEN entera | Servidor Postgres | Rechazar  | Web adminer        |

Esta regla tiene como objetivo bloquear el acceso a la interfaz web de administración de bases de datos “Web adminer” desde cualquier equipo de la red GREEN.

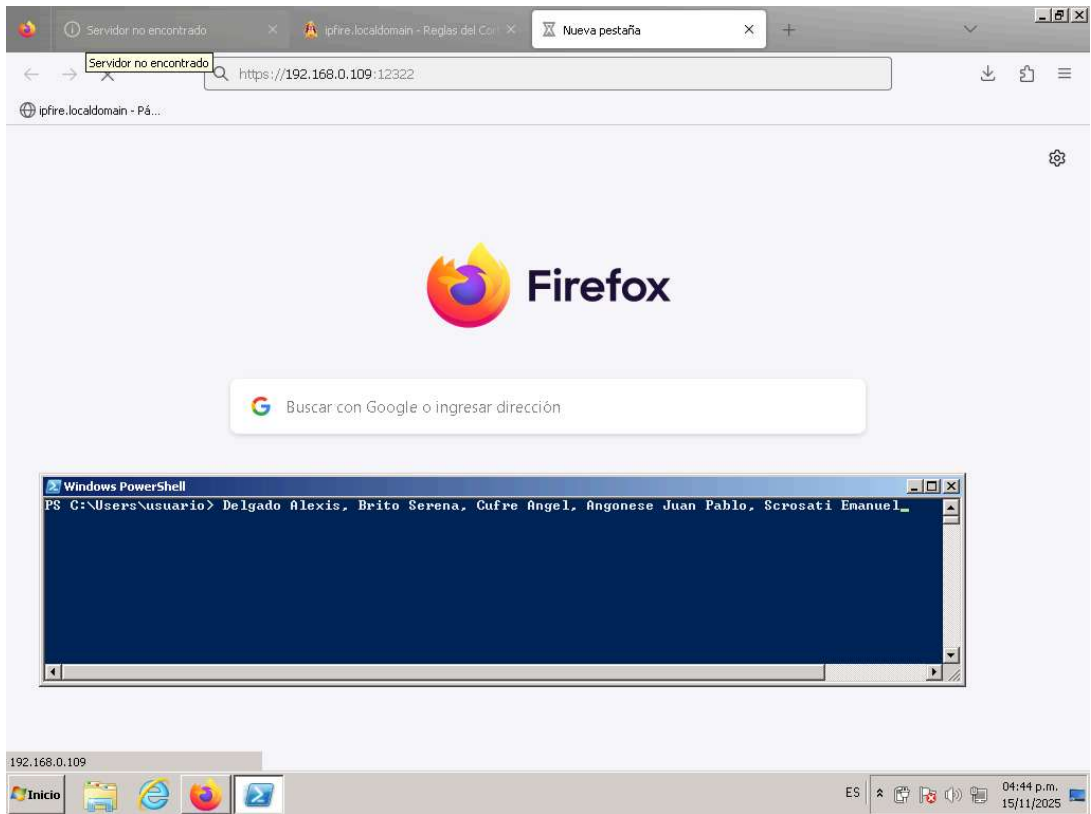
Puerto involucrado→12322 (TCP)

Antes de aplicar la regla accedemos a la interfaz de administración web Adminer mediante el navegador, utilizando la dirección <https://192.168.0.109:12322/> :



Corroboramos el ingreso exitoso.

Luego de aplicar la regla:



La conexión falla al intentar acceder al servicio en el puerto correspondiente, lo que indica que la regla aplicada en el firewall está funcionando correctamente. Este comportamiento confirma que el tráfico ha sido filtrado según lo establecido, impidiendo el acceso desde la red GREEN al servicio especificado.

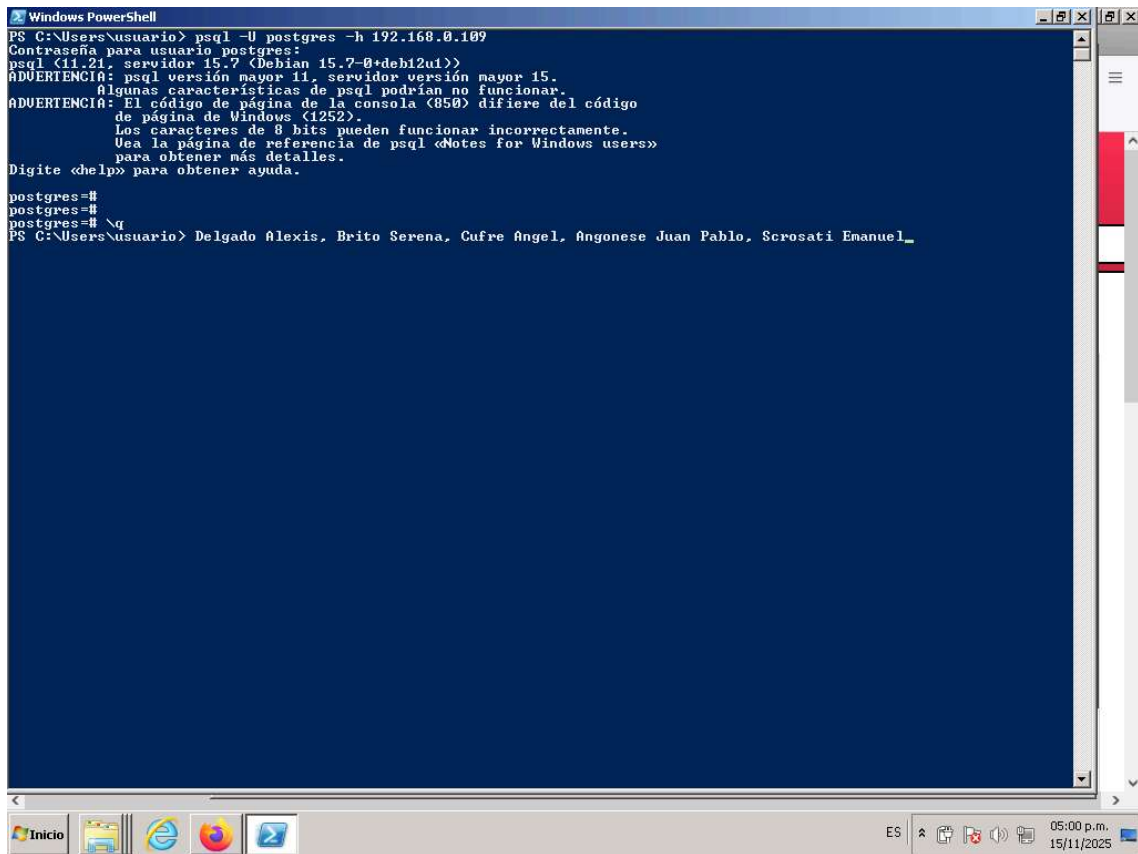
### Regla 9

| Origen           | Destino           | Condición | Servicio/Protocolo |
|------------------|-------------------|-----------|--------------------|
| Red GREEN entera | Servidor Postgres | Rechazar  | BD Postgres        |

Esta regla tiene como objetivo bloquear el acceso al servicio de base de datos PostgreSQL desde cualquier equipo de la red GREEN.

Puerto involucrado→5432(TCP)

Verificamos antes de aplicar la regla mediante el siguiente comando “psql -U postgres -h 192.168.0.189” :

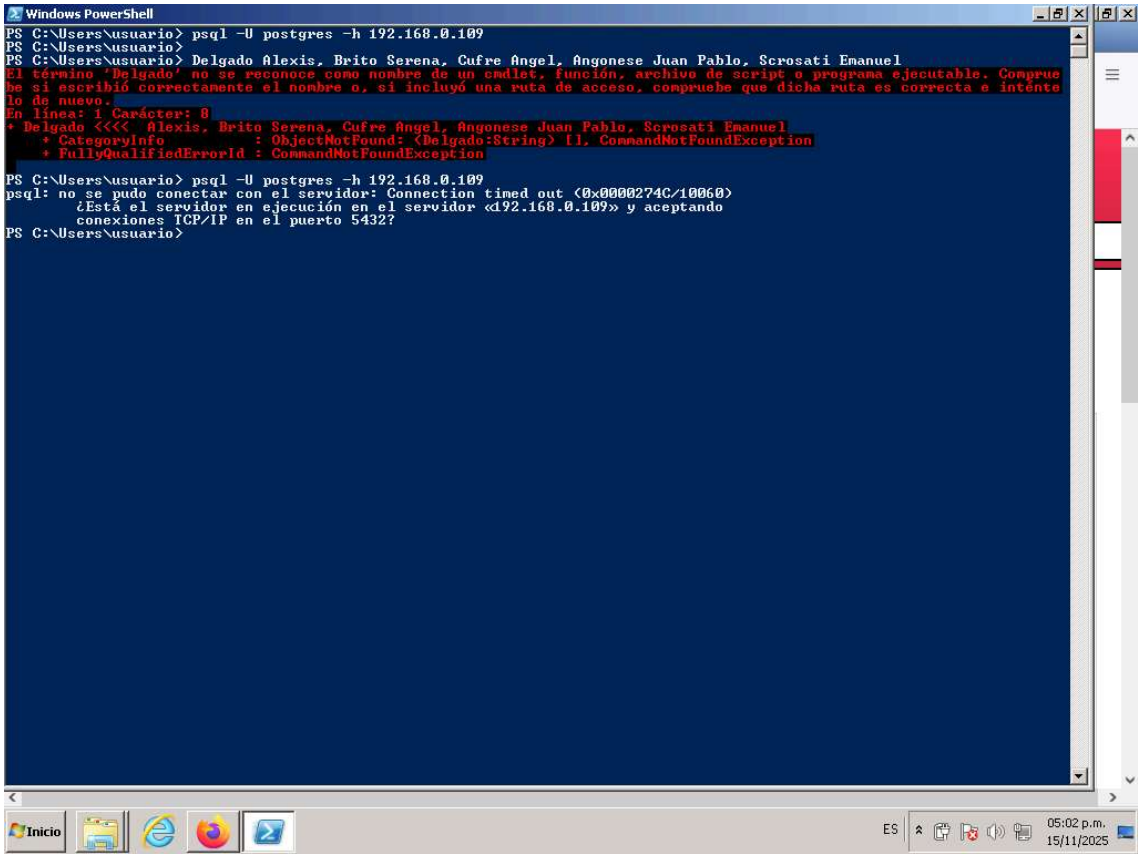


```
Windows PowerShell
PS C:\Users\usuario> psql -U postgres -h 192.168.0.189
Contraseña para usuario postgres:
psql (11.21, servidor 15.7 (Debian 15.7-0+deb12u1))
ADVERTENCIA: psql versión mayor 11, servidor versión mayor 15.
Algunas características de psql podrían no funcionar.
ADVERTENCIA: El código de página de la consola (850) difiere del código
de página de Windows (1252).
Los caracteres de 8 bits pueden funcionar incorrectamente.
Uea la página de referencia de psql «Notes for Windows users»
para obtener más detalles.
Digite «help» para obtener ayuda.

postgres=#
postgres=#
postgres=# \q
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel_
```

La conexión se establece correctamente.

Luego de aplicar la regla repetimos el intento utilizando el mismo comando:



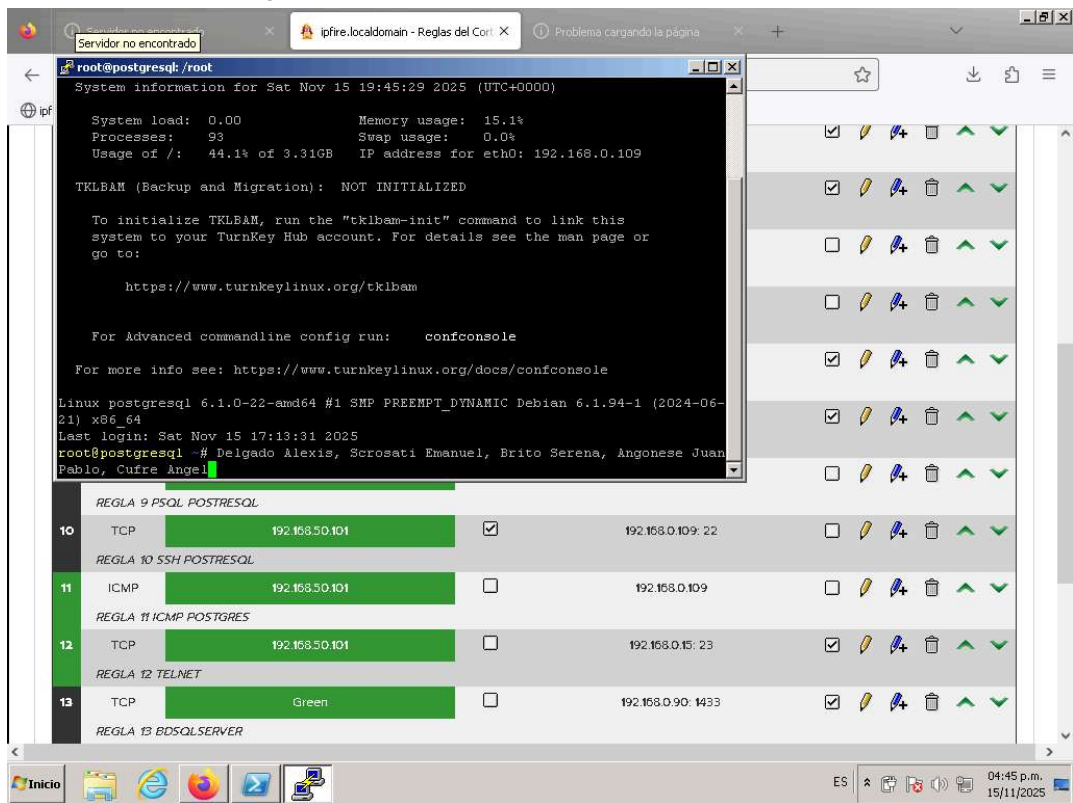
Regla 10

| Origen                 | Destino           | Condición | Servicio/Protocolo |
|------------------------|-------------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor Postgres | Rechazar  | SSH                |

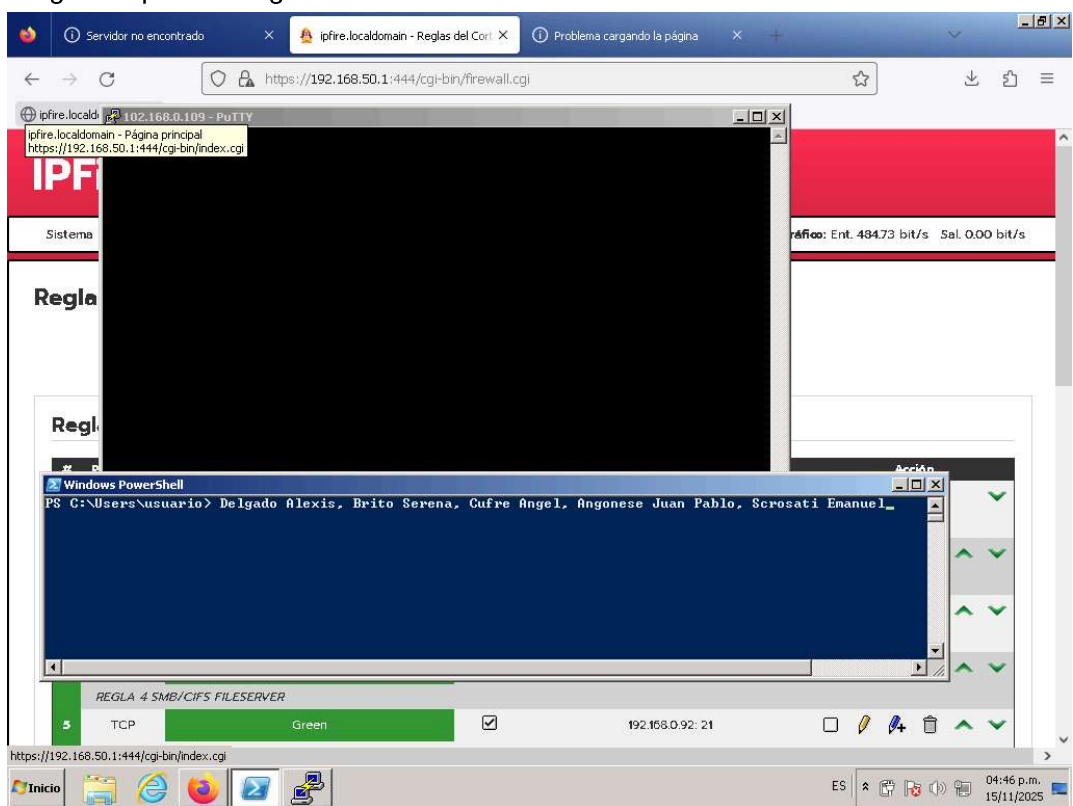
Esta regla tiene como objetivo bloquear el acceso remoto por SSH desde una máquina específica de la red GREEN hacia el servidor PostgreSQL.



Antes de aplicar la regla:



Luego de aplicar la regla:



\*se adjunta video

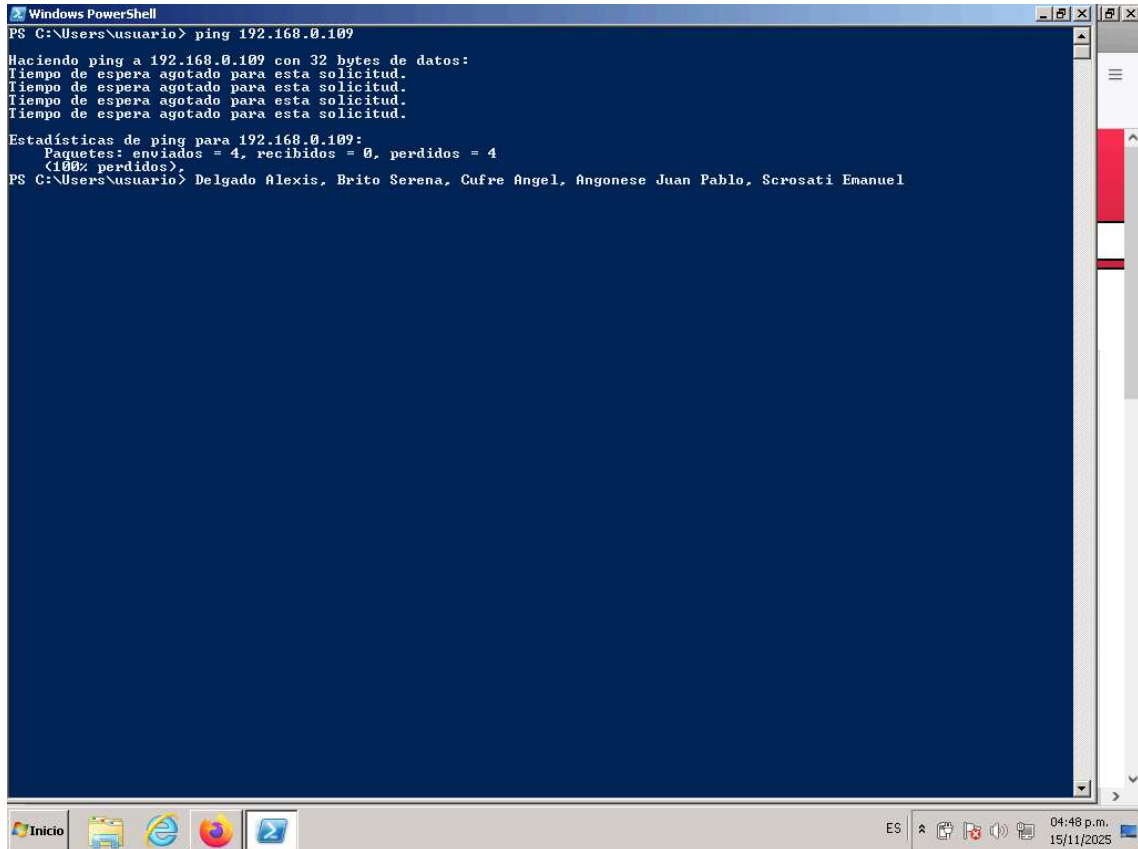
## Regla 11

| Origen                 | Destino           | Condición | Servicio/Protocolo |
|------------------------|-------------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor Postgres | Permitir  | ICMP               |

Esta regla tiene como objetivo permitir que una IP específica de la red GREEN pueda hacer ping(protocolo ICMP) al servidor Postgres.

En este caso, antes de aplicar la regla, aplicamos una política restrictiva en el firewall para poder corroborar el correcto funcionamiento de la misma.

Antes de aplicar la regla:



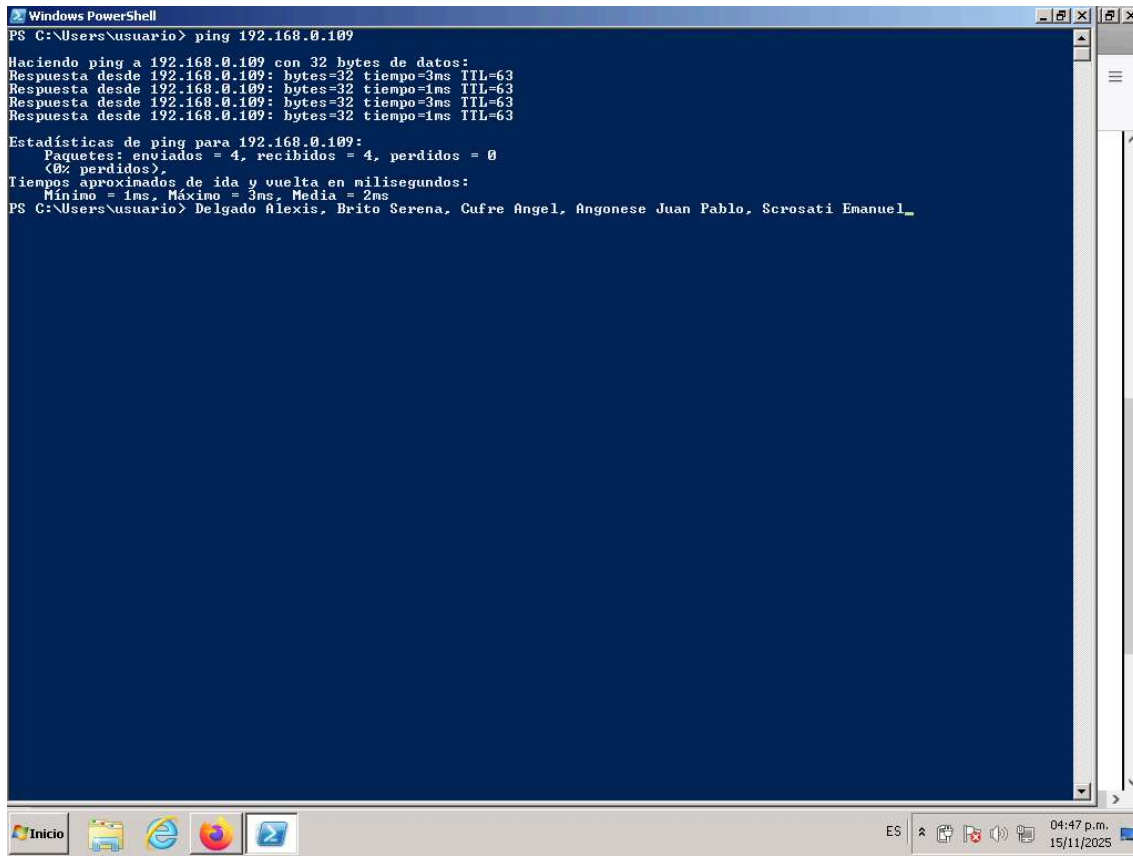
```
Windows PowerShell
PS C:\Users\usuario> ping 192.168.0.109

Haciendo ping a 192.168.0.109 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.109:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos).
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel
```

The screenshot shows a Windows PowerShell terminal window. The user has entered the command 'ping 192.168.0.109'. The output shows four 'Tiempo de espera agotado para esta solicitud.' (Timeout for this request) messages, indicating that the ping failed. Below this, the statistics for the ping are shown: 'Paquetes: enviados = 4, recibidos = 0, perdidos = 4' (Packets: sent = 4, received = 0, lost = 4) and '(100% perdidos)' (100% lost). The window title is 'Windows PowerShell' and the taskbar at the bottom shows the Start button and several application icons. The system clock in the bottom right corner indicates the time is 04:48 p.m. on 15/11/2025.

Luego de aplicar la regla:



```
Windows PowerShell
PS C:\Users\usuario> ping 192.168.0.109

Haciendo ping a 192.168.0.109 con 32 bytes de datos:
Respuesta desde 192.168.0.109: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.0.109: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.0.109: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.0.109: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 192.168.0.109:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 3ms, Media = 2ms
PS C:\Users\usuario> Delgado Alexis, Brito Serena, Cufre Angel, Angonese Juan Pablo, Scrosati Emanuel_
```

*\*se adjunta video*

## Regla 12

| Origen                 | Destino         | Condición | Servicio/Protocolo |
|------------------------|-----------------|-----------|--------------------|
| IP de un cliente GREEN | Servidor Telnet | Permitir  | Telnet             |

Esta regla tiene como objetivo habilitar el acceso al servicio Telnet (puerto 23) desde una máquina específica de la red GREEN. En este caso se aplica una dirección IP para simular el servidor Telnet.

IP asignado al servidor Telnet→ 192.168.0.15

## Regla 13

| Origen           | Destino               | Condición | Servicio/Protocolo |
|------------------|-----------------------|-----------|--------------------|
| Red GREEN entera | Servidor BD SqlServer | Rechazar  | BD SqlServer       |

Esta regla tiene como objetivo bloquear el acceso al servicio de base de datos SQL Server (puerto 1433) desde cualquier equipo de la red GREEN. En este caso se aplica una dirección IP para simular el Servidor BD SqlServer.

IP asignado al Servidor BD SqlServer → 192.168.0.90

#### Regla 14

| <b>Origen</b>    | <b>Destino</b> | <b>Condición</b> | <b>Servicio/Protocolo</b> |
|------------------|----------------|------------------|---------------------------|
| Red GREEN entera | Servidor NTP   | Permitir         | NTP                       |

Esta regla tiene como objetivo autorizar al servidor NTP (Protocolo de Tiempo de Red) (puerto 123) es un servidor que sincroniza la hora de dispositivos en una red con la hora exacta, utilizando el protocolo NTP. Esta regla habilita que los equipos de la red GREEN puedan sincronizar su hora con el servidor NTP. En este caso se aplica una dirección IP para simular el servidor NTP.

IP asignado al NTP → 192.168.0.93

#### Regla 15

| <b>Origen</b>    | <b>Destino</b>    | <b>Condición</b> | <b>Servicio/Protocolo</b> |
|------------------|-------------------|------------------|---------------------------|
| Red GREEN entera | Servidor BD Mysql | Permitir         | BD Mysql                  |

Esta regla tiene como objetivo autorizar a el acceso al al servicio de base de datos MySQL (puerto 3306) desde cualquier equipo de la red GREEN. En este caso se aplica una dirección IP para simular el servidor Telnet.

IP asignado al Servidor MySQL → 192.168.0.94

Reglas configuradas:

ipfire.localdomain - Reglas del Cort...EDB: Open-Source, Enterprise Poi...Firefox View

https://192.168.50.1:444/cgi-bin/firewall.cgiipfire.localdomain - Pá...

Reglas del Cortafuegos

| #                              | Protocolo: | Origen         | Registro                            | Destino               | Acción                              |
|--------------------------------|------------|----------------|-------------------------------------|-----------------------|-------------------------------------|
| 1                              | TCP        | 192.168.50.101 | <input checked="" type="checkbox"/> | 192.168.0.237: 12322  | <input checked="" type="checkbox"/> |
| REGLA 1 WEBADMINER LAMP        |            |                |                                     |                       |                                     |
| 2                              | TCP        | Green          | <input checked="" type="checkbox"/> | 192.168.0.237: 22     | <input checked="" type="checkbox"/> |
| REGLA 2 SSH LAMP               |            |                |                                     |                       |                                     |
| 3                              | ICMP       | 192.168.50.101 | <input type="checkbox"/>            | 192.168.0.237         | <input checked="" type="checkbox"/> |
| REGLA 3 ICMP LAMP              |            |                |                                     |                       |                                     |
| 4                              | TCP        | Green          | <input checked="" type="checkbox"/> | 192.168.0.92: 139,445 | <input checked="" type="checkbox"/> |
| REGLA 4 SMB/CIFS FILESERVER    |            |                |                                     |                       |                                     |
| 5                              | TCP        | Green          | <input checked="" type="checkbox"/> | 192.168.0.92: 21      | <input checked="" type="checkbox"/> |
| REGLA 5 FTP FILESERVER         |            |                |                                     |                       |                                     |
| 6                              | TCP        | 192.168.50.101 | <input type="checkbox"/>            | 192.168.0.92: 22      | <input checked="" type="checkbox"/> |
| REGLA 6 SSH FILSERVER          |            |                |                                     |                       |                                     |
| 7                              | ICMP       | Green          | <input type="checkbox"/>            | 192.168.0.92          | <input checked="" type="checkbox"/> |
| REGLA 7 ICMP FILESERVER        |            |                |                                     |                       |                                     |
| 8                              | TCP        | Green          | <input type="checkbox"/>            | 192.168.0.109: 12322  | <input checked="" type="checkbox"/> |
| REGLA 8 WEB ADMINER POSTGRESQL |            |                |                                     |                       |                                     |
| 9                              | TCP        | Green          | <input type="checkbox"/>            | 192.168.0.109: 5432   | <input checked="" type="checkbox"/> |
| REGLA 9 PSQL POSTRESQL         |            |                |                                     |                       |                                     |

Inicio

ES

05:11 p.m.  
15/11/2025

ipfire.localdomain - Reglas del Cortafuegos

EDB: Open-Source, Enterprise Po... X

https://192.168.50.1:444/cgi-bin/firewall.cgi

ipfire.localdomain - Pá...

| Regla                          | Protocolo | Estado         | Acción                              | IP/Porto             | Activo                              | Editar | Eliminar | Subir | Bajar |
|--------------------------------|-----------|----------------|-------------------------------------|----------------------|-------------------------------------|--------|----------|-------|-------|
| 8                              | TCP       | Green          | <input type="checkbox"/>            | 192.168.0.109: 12322 | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 8 WEB ADMINER POSTGRESQL |           |                |                                     |                      |                                     |        |          |       |       |
| 9                              | TCP       | Green          | <input type="checkbox"/>            | 192.168.0.109: 5432  | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 9 PSQL POSTRESQL         |           |                |                                     |                      |                                     |        |          |       |       |
| 10                             | TCP       | 192.168.50.101 | <input checked="" type="checkbox"/> | 192.168.0.109: 22    | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 10 SSH POSTRESQL         |           |                |                                     |                      |                                     |        |          |       |       |
| 11                             | ICMP      | 192.168.50.101 | <input type="checkbox"/>            | 192.168.0.109        | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 11 ICMP POSTGRES         |           |                |                                     |                      |                                     |        |          |       |       |
| 12                             | TCP       | 192.168.50.101 | <input type="checkbox"/>            | 192.168.0.15: 23     | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 12 TELNET                |           |                |                                     |                      |                                     |        |          |       |       |
| 13                             | TCP       | Green          | <input type="checkbox"/>            | 192.168.0.90: 1433   | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 13 BDSQLSERVER           |           |                |                                     |                      |                                     |        |          |       |       |
| 14                             | UDP       | Green          | <input checked="" type="checkbox"/> | 192.168.0.93: 123    | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 14 NTP                   |           |                |                                     |                      |                                     |        |          |       |       |
| 15                             | TCP       | Green          | <input checked="" type="checkbox"/> | 192.168.0.94: 3306   | <input checked="" type="checkbox"/> |        |          |       |       |
| REGLA 15 BDMYSQL               |           |                |                                     |                      |                                     |        |          |       |       |

Green > Internet (Permitido)

Política: Permitido

Inicio

ES 05:11 p.m. 15/11/2025