Firewall de Linux

24/10/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Vemos el sistema operativo

```
[root@localhost ~]# cat /etc/redhat-release
Fedora release 38 (Thirty Eight)
[root@localhost ~]# cat /etc/redhat-release _
```

Vemos el estado del firewall

```
[root@localhost ~]# firewall-cmd --state
running
[root@localhost ~]#
```

También lo podemos ver con este comando

```
[root@localhost ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
    Drop-In: /usr/lib/systemd/system/service.d
             └─10-timeout-abort.conf
     Active: active (running) since Mon 2023-10-23 16:03:35 CEST; 1h 17min ago
       Docs: man:firewalld(1)
   Main PID: 743 (firewalld)
      Tasks: 4 (limit: 2293)
     Memory: 46.6M
        CPU: 2.760s
     CGroup: /system.slice/firewalld.service
             └─743 /usr/bin/python3 -sP /usr/sbin/firewalld --nofork --nopid

oct 23 16:03:34 localhost systemd[1]: Starting firewalld.service - firewalld - dynamic firewall daemon...
oct 23 16:03:35 localhost systemd[1]: Started firewalld.service - firewalld - dynamic firewall daemon.
[root@localhost ~]#
```

Listamos la zona del firewall

```
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

FedoraWorkstation
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client samba-client ssh
  ports: 1025-65535/udp 1025-65535/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

dmz
  target: default
  icmp-block-inversion: no
  interfaces:
--Más--
```

Lo hacemos con el comando firewall-cmd –list-all-zones |more

```
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client mdns ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
--Más--
```

Vemos la zona por defecto

```
[root@localhost ~]# firewall-cmd --get-default-zone
FedoraServer
[root@localhost ~]#
```

Vemos las zonas activas

```
[root@localhost ~]# firewall-cmd --get-default-zone
FedoraServer
[root@localhost ~]# firewall-cmd --get-active-zones
FedoraServer
  interfaces: enp0s3
[root@localhost ~]# _
```

Lista de todos los ajustes de la zona publica

```
[root@localhost ~]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

Hacemos ping de las dos maquinas

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.68.16.75  netmask 255.255.252.0  broadcast 10.68.19.255
        inet6 fe80::a00:27ff:fe0b:f0ff  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0b:f0:ff  txqueuelen 1000  (Ethernet)
        RX packets 110543  bytes 7374833 (7.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1357  bytes 113333 (110.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 15  bytes 1768 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1768 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# ping 10.68.18.178
PING 10.68.18.178 (10.68.18.178) 56(84) bytes of data.
64 bytes from 10.68.18.178: icmp_seq=1 ttl=128 time=0.432 ms
64 bytes from 10.68.18.178: icmp_seq=2 ttl=128 time=0.785 ms
64 bytes from 10.68.18.178: icmp_seq=3 ttl=128 time=0.682 ms
64 bytes from 10.68.18.178: icmp_seq=4 ttl=128 time=0.857 ms
64 bytes from 10.68.18.178: icmp_seq=5 ttl=128 time=0.368 ms
64 bytes from 10.68.18.178: icmp_seq=6 ttl=128 time=0.947 ms
^C
--- 10.68.18.178 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4995ms
rtt min/avg/max/mdev = 0.368/0.678/0.947/0.213 ms
[root@localhost ~]#
```

```
PS C:\> ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : madrid.fusp.ceu
   Vínculo: dirección IPv6 local. . . : fe80::3ddb:4ae4:47cf:8f66%7
   Dirección IPv4. . . . . . . . . . . . . . : 10.68.18.178
   Máscara de subred . . . . . . . . . . . . : 255.255.252.0
   Puerta de enlace predeterminada . . . . . : 10.68.16.1

Adaptador de Ethernet VirtualBox Host-Only Network:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::c740:a16a:cec2:94c9%10
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
PS C:\> ping 10.68.16.75

Haciendo ping a 10.68.16.75 con 32 bytes de datos:
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.68.16.75:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\>
```

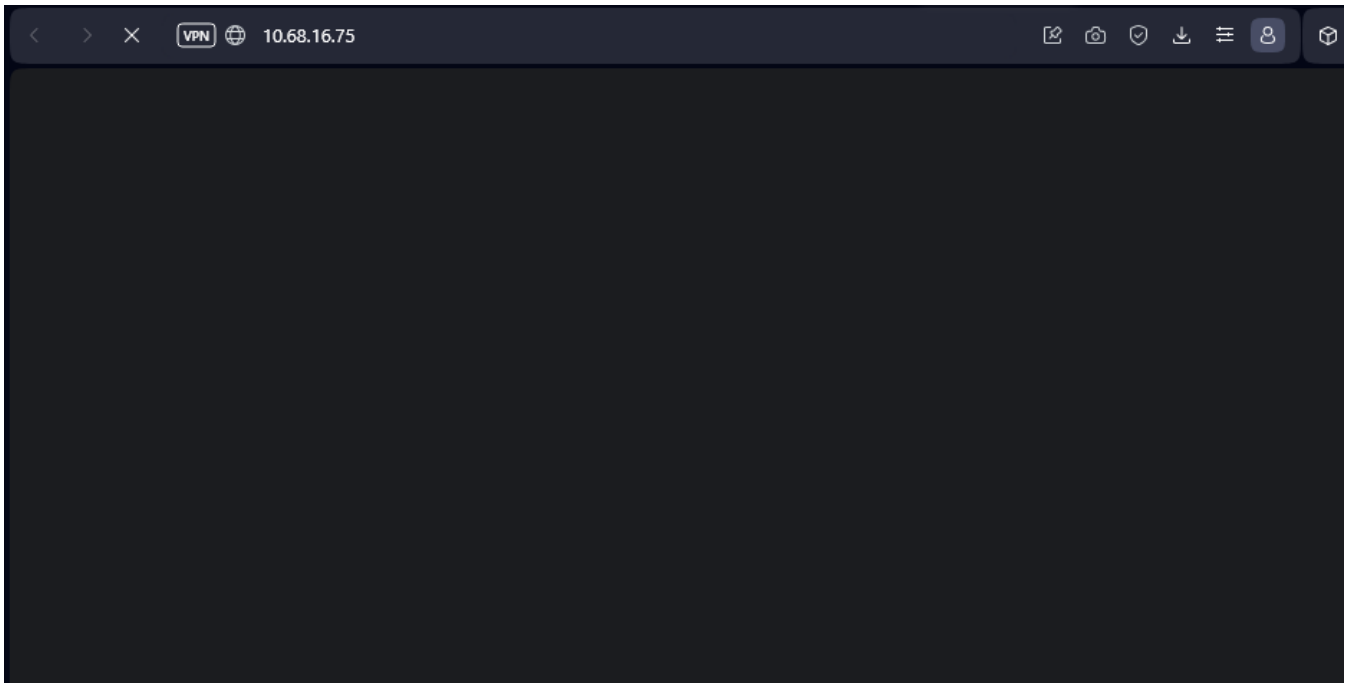
Vemos el estado de httpd

```
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
    Drop-In: /usr/lib/systemd/system/service.d
             └─10-timeout-abort.conf
     Active: active (running) since Mon 2023-10-23 18:17:51 CEST; 3s ago
       Docs: man:httpd.service(8)
   Main PID: 1770 (httpd)
     Status: "Started, listening on: port 80"
      Tasks: 177 (limit: 2293)
     Memory: 14.3M
        CPU: 193ms
     CGroup: /system.slice/httpd.service
             ├─1770 /usr/sbin/httpd -DFOREGROUND
             ├─1771 /usr/sbin/httpd -DFOREGROUND
             ├─1772 /usr/sbin/httpd -DFOREGROUND
             ├─1773 /usr/sbin/httpd -DFOREGROUND
             └─1774 /usr/sbin/httpd -DFOREGROUND

oct 23 18:17:51 localhost.localdomain systemd[1]: Starting httpd.service - The Apache HTTP Server...
oct 23 18:17:51 localhost.localdomain httpd[1770]: AH00558: httpd: Could not reliably determine the server's fully quali
oct 23 18:17:51 localhost.localdomain httpd[1770]: Server configured, listening on: port 80
oct 23 18:17:51 localhost.localdomain systemd[1]: Started httpd.service - The Apache HTTP Server.
lines 1-22/22 (END)
```

Esta activo

El servicio no esta activo



Activamos el servicio de httpd

```
[root@localhost ~]# firewall-cmd --add-service=http --permanent
success
[root@localhost ~]# _
```

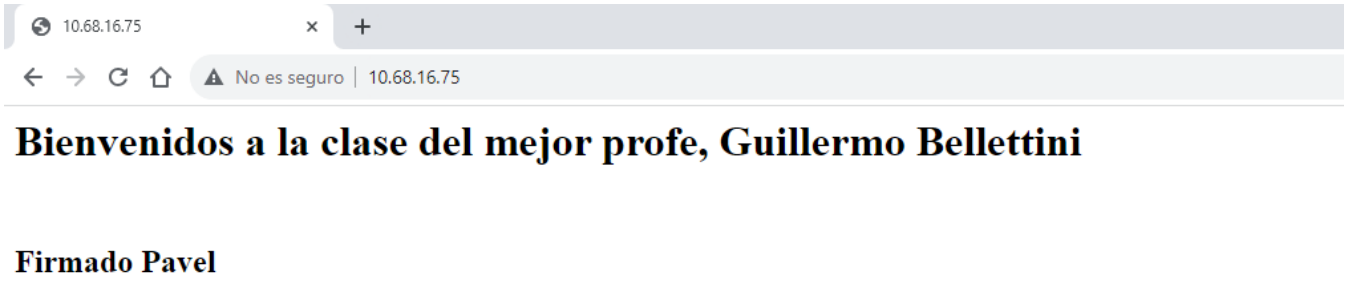
Recargamos el servicio

```
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# _
```

Listamos otra vez y ahora si nos sale

```
[root@localhost ~]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client http ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

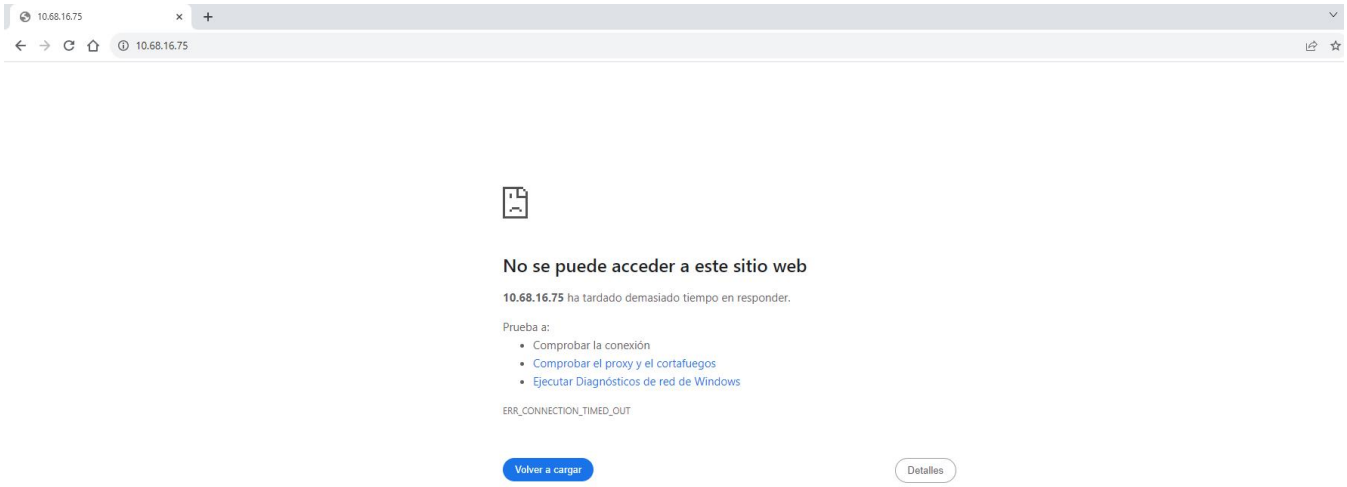
Podemos acceder a la pagina



Quitamos el servicio

```
[root@localhost html]# firewall-cmd --add-service=http --permanent
Warning: ALREADY_ENABLED: http
success
[root@localhost html]# firewall-cmd --remove-service=http --permanent
success
[root@localhost html]# firewall-cmd --reload
success
[root@localhost html]# _
```

Ya no podemos acceder a la pagina



Bloqueamos el ping

```
[root@localhost html]# firewall-cmd --zone=FedoraServer --add-icmp-block-inversion --permanent
success
[root@localhost html]# firewall-cmd --reload
success
[root@localhost html]# _
```

Listamos los servicios

```
[root@localhost html]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: yes
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost html]# _
```

Icmp-block-inversion: yes

Ya no hacemos ping

```
PS C:\> ping 10.68.16.75

Haciendo ping a 10.68.16.75 con 32 bytes de datos:
Respuesta desde 10.68.16.75: Red de destino inaccesible.
Respuesta desde 10.68.16.75: Red de destino inaccesible.
Respuesta desde 10.68.16.75: Red de destino inaccesible.
Respuesta desde 10.68.16.75: Red de destino inaccesible.

Estadísticas de ping para 10.68.16.75:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
PS C:\>
```

Quitamos el bloqueo de ping

```
[root@localhost html]# firewall-cmd --zone=FedoraServer --remove-icmp-block-inversion --permanent
success
[root@localhost html]# firewall-cmd --reload
success
[root@localhost html]#
```

Ya hacemos ping

```
PS C:\> ping 10.68.16.75

Haciendo ping a 10.68.16.75 con 32 bytes de datos:
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.68.16.75: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.68.16.75:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
PS C:\>
```

Listamos

```
[root@localhost html]# firewall-cmd --list-all
FedoraServer (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ntp ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost html]#
```

Vemos la configuración del panico

```
[root@localhost html]# firewall-cmd --query-panic
no
[root@localhost html]# _
```