

# Firewall UFW – FIREWALLD

Le firewall UFW nativement sous Debian mais peut être installé sous RH/CentOs également

```
root@debian12:/proc/sys/crypto# ufw enable
Firewall is active and enabled on system startup
root@debian12:/proc/sys/crypto#
root@debian12:/proc/sys/crypto# ufw disable
Firewall stopped and disabled on system startup
root@debian12:/proc/sys/crypto#
root@debian12:/proc/sys/crypto# ufw enable
Firewall is active and enabled on system startup
root@debian12:/proc/sys/crypto#
root@debian12:/proc/sys/crypto# ufw status
Status: active
root@debian12:/proc/sys/crypto#
root@debian12:/proc/sys/crypto# ufw app list
Available applications:
  AIM
  Bonjour
  CIFS
  CUPS
  DNS
  Deluge
  IMAP
  IMAPS
  IPP
  KTorrent
  Kerberos Admin
  Kerberos Full
  Kerberos KDC
```

```
root@debian12:/proc/sys/crypto# ufw reject ssh
```

```
Rule added
```

```
Rule added (v6)
```

```
root@debian12:/proc/sys/crypto#
```

```
root@debian12:/proc/sys/crypto# ufw status numbered
```

```
Status: active
```

To	Action	From
--	-----	----
[ 1] 22/tcp	REJECT IN	Anywhere
[ 2] 22/tcp (v6)	REJECT IN	Anywhere (v6)

```
root@debian12:/proc/sys/crypto#
```

```
root@debian12:/proc/sys/crypto# ufw reject out ssh
```

```
Rule added
```

```
Rule added (v6)
```

```
root@debian12:/proc/sys/crypto#
```

```
root@debian12:/proc/sys/crypto# ufw status numbered
```

```
Status: active
```

To	Action	From	
--	-----	----	
[ 1] 22/tcp	REJECT IN	Anywhere	
[ 2] 22/tcp	REJECT OUT	Anywhere	(out)
[ 3] 22/tcp (v6)	REJECT IN	Anywhere (v6)	
[ 4] 22/tcp (v6)	REJECT OUT	Anywhere (v6)	(out)

```
root@debian12:/proc/sys/crypto# █
```

```
root@debian12:/proc/sys/crypto# ufw status numbered
Status: active
```

To	Action	From	
--	-----	----	
[ 1] 22/tcp	REJECT IN	Anywhere	
[ 2] 22/tcp	REJECT OUT	Anywhere	(out)
[ 3] 22/tcp (v6)	REJECT IN	Anywhere (v6)	
[ 4] 22/tcp (v6)	REJECT OUT	Anywhere (v6)	(out)

```
root@debian12:/proc/sys/crypto# ufw delete 1
```

```
Deleting:
  reject 22/tcp
Proceed with operation (y|n)? y
Rule deleted
```

```
root@debian12:/proc/sys/crypto#
root@debian12:/proc/sys/crypto# ufw reset
```

```
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250110_142300'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250110_142300'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250110_142300'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250110_142300'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250110_142300'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250110_142300'
```

```
root@debian12:/proc/sys/crypto# █
```

```

root@debian12:/var/log# ufw logging on
Logging enabled
root@debian12:/var/log#
root@debian12:/var/log# █

```

Installation sous CentOs 9

```
Activités Terminal 10 janv. 14:46
root@device-58:~
[root@device-58 ~]# systemctl stop firewalld.service
[root@device-58 ~]#
[root@device-58 ~]# **yum install epel-release
bash: **yum: command not found...
[root@device-58 ~]#
[root@device-58 ~]# **yum install --enablerepo="epel" ufw
bash: **yum: command not found...
[root@device-58 ~]#
[root@device-58 ~]# ufw enable
Le pare-feu est actif et lancé au démarrage du système
[root@device-58 ~]#
[root@device-58 ~]# ufw allow ssh
La règle a été ajoutée
La règle a été ajoutée (v6)
[root@device-58 ~]# ufw status numbered
État : actif

    Vers                Action          De
    ----                -
[ 1] SSH                ALLOW IN       Anywhere
[ 2] 224.0.0.251 mDNS   ALLOW IN       Anywhere
[ 3] 22                 ALLOW IN       Anywhere
[ 4] SSH (v6)          ALLOW IN       Anywhere (v6)
[ 5] ff02::fb mDNS     ALLOW IN       Anywhere (v6)
[ 6] 22 (v6)           ALLOW IN       Anywhere (v6)

[root@device-58 ~]#
```

SEMANAGE SELinux RH

```
root@device-58:~
[root@device-58 ~]# systemctl stop sshd.service
[root@device-58 ~]#
[root@device-58 ~]# semanage port -l | grep ssh
ssh_port_t                                tcp                2222, 22
[root@device-58 ~]#
[root@device-58 ~]# semanage port -a -t ssh_port_t -p tcp 2222
ValueError: Le port tcp/2222 est déjà défini
[root@device-58 ~]#
[root@device-58 ~]# firewall-cmd --permanent --zone=public --add-port=2222/tcp
Warning: ALREADY_ENABLED: 2222:tcp
success
[root@device-58 ~]#
[root@device-58 ~]# firewall-cmd --reload
success
[root@device-58 ~]#
[root@device-58 ~]# grep Port /etc/ssh/sshd_config
Port 2222
#GatewayPorts no
[root@device-58 ~]#
[root@device-58 ~]# systemctl start sshd.service
[root@device-58 ~]#
[root@device-58 ~]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-01-10 15:24:50 CET; 6s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 3312 (sshd)
    Tasks: 1 (limit: 36711)
   Memory: 1.7M
      CPU: 14ms
   CGroup: /system.slice/sshd.service
           └─3312 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

janv. 10 15:24:50 device-58.home systemd[1]: Starting OpenSSH server daemon...
janv. 10 15:24:50 device-58.home sshd[3312]: Server listening on 0.0.0.0 port 2222.
janv. 10 15:24:50 device-58.home sshd[3312]: Server listening on :: port 2222.
janv. 10 15:24:50 device-58.home systemd[1]: Started OpenSSH server daemon.
lines 1-16/16 (END)
```