UFW un pare-feu facile

- Objet : Configurer le pare-feu linux (Iptable) simplement
- Niveau requis :
  débutant, avisé
- Commentaires : *Cette petite présentation a pour but de mettre en place quelques mesures de sécurité pour votre ordinateur. Cela ne prendra pas plus de 5 minutes.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !
- Suivi :
  - Création par martin_mtl le 10/12/2012
  - Testé par deuchdeb le 29/12/2017
- Commentaires sur le forum : C'est ici[1)]

Installation

C'est tout simple dans un terminal administrateur entrer la commande suivante:

```
apt-get update && apt-get install ufw
```

Utilisation

Syntaxe de base

Mettre en route le pare-feu

Si vous n'avez qu'un accès ssh, surtout assurez-vous avant de démarrer ufw que les règles de ce dernier ne bloque pas SSH (port 22 par défaut) sans quoi votre session ssh cessera et vous ne pourrez plus vous connecter via ssh

```
ufw enable
```

ce qui donne:

```
ufw enable
```

commande interactive

```
Command may disrupt existing ssh connections. Proceed with operation
(y|n)?
```

Ce qui veut dire que la connexion SSH peut être interrompue… Pour tout laisser passer avant de

démarrer ufw

```
ufw default allow
```

Cela revient à ne pas avoir de pare-feu mais vous serez certain de ne pas avoir votre connexion SSH coupé. il faudra obligatoirement définir les règles d'ufw après son démarrage

Après de démarrage d'ufw vous pouvez consulter son état et les règles qu'il applique

```
ufw status verbose
```

retour de la commande

```
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing)
New profiles: skip
```

Ici Tout passe!

Arrêter le pare-feu

```
ufw disable
```

Autoriser toutes les connections par défaut

```
ufw default allow
```

Refuser toutes les connections par défaut

Attention si votre unique accès passe par ssh vous serez déconnecté!

```
ufw default deny
```

Autoriser le trafic sur un port

```
ufw allow port
```

Bloquer un port

```
ufw deny port
```

Connaître le numéro d'une règle

```
ufw status numbered
```

Supprimer une règle

```
ufw delete <numéro-de-la-règle>
```

Vérifier l'état du pare-feu

```
ufw status
```

```
ufw status verbose (plus d'info sont fournies)
```

Configuration de base du pare feu

Entrer la commande suivante:

```
ufw enable
```

> Une fois que le pare-feu est en route, il l'est toujours. Vous pouvez éteindre l'ordinateur au prochain démarrage le pare feu sera actif

La politique par défaut est la suivante, on autorise les connections sortantes et on interdit les connections entrantes.

Si vous entrez la commande suivante:

```
ufw status verbose
```

Vous aurez ceci comme réponse:

retour de la commande

```
    Status: active
    02.Logging: on (low)
    03.Default: deny (incoming), allow (outgoing)
    04.New profiles: skip
```

Vous avez ainsi la configuration de base

Pour interdire le ping (ICMP Echo Request), il faut commenter la ligne suivante dans le fichier `/etc/ufw/before.rules`:

```
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
```

Voir : nano

Exemple de configuration avancée

On met en route le pare-feu

```
ufw enable
```

On bloque tout (rien ne sort, rien ne rentre)

```
ufw default deny incoming
```

```
ufw default deny outgoing
```

On active la journalisation

```
ufw logging on
```

On autorise ensuite les services dont on à besoin

Voir le fichier `/etc/services` en bas de cette page.

Autoriser l'accès en sortie à un serveur ssh

```
ufw allow out 22/tcp
```

Autoriser l'accès en entré (comprendre de l'extérieur) à un serveur ssh

```
ufw allow in 22/tcp
```

Pour autoriser l’accès en sortie à internet

```
ufw allow out 80/tcp
```

```
ufw allow out 53/udp
```

```
ufw allow out 443/tcp
```

Autoriser l’accès en sortie à un serveur ftp

```
ufw allow out 20/tcp
```

```
ufw allow out 21/tcp
```

Autoriser l’accès en sortie à la messagerie

smtp

```
ufw allow out 25/tcp
```

pop3

```
ufw allow out 110/tcp
```

pop3 sécurisé

```
ufw allow out 995/tcp
```

imap2

```
ufw allow out 143/tcp
```

imap3

```
ufw allow out  220/tcp
```

Autoriser en sortie amule

```
ufw allow out  4662/tcp
```

```
ufw allow out  4665/udp
```

```
ufw allow out  4672/udp
```

Autoriser en sortie bittorent

```
ufw allow out 6880:6999/tcp
```

```
ufw allow out 6880:6999/udp
```

Autoriser en sortie irc

```
ufw allow out 194/tcp
```

Autoriser en sortie freenode

```
ufw allow out 6667/tcp
```

Pour appliquer les changements

```
ufw disable && ufw enable
```

Pour supprimer une règle

```
ufw delete allow out 80/tcp
```

Le fichier /etc/services

/etc/services

```
cpmux       1/tcp                # TCP port service multiplexer echo
                7/tcp
echo        7/udp
discard     9/tcp        sink null
discard     9/udp        sink null
systat      11/tcp        users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp        quote
msp     18/tcp                # message send protocol
msp     18/udp
chargen     19/tcp        ttytst source
chargen     19/udp        ttytst source
ftp-data    20/tcp
ftp     21/tcp
```

```
fsp     21/udp        fspd
ssh     22/tcp                # SSH Remote Login Protocol
ssh     22/udp
telnet      23/tcp
smtp        25/tcp        mail
time        37/tcp        timserver
time        37/udp        timserver
rlp     39/udp        resource    # resource location
nameserver  42/tcp        name        # IEN 116
whois       43/tcp        nicname
tacacs      49/tcp                # Login Host Protocol (TACACS)
tacacs      49/udp
re-mail-ck  50/tcp                # Remote Mail Checking Protocol
re-mail-ck  50/udp
domain      53/tcp                # name-domain server
domain      53/udp
mtp     57/tcp                # deprecated
tacacs-ds   65/tcp                # TACACS-Database Service
tacacs-ds   65/udp
bootps      67/tcp                # BOOTP server
bootps      67/udp
bootpc      68/tcp                # BOOTP client
bootpc      68/udp
tftp        69/udp
gopher      70/tcp                # Internet Gopher
gopher      70/udp
rje     77/tcp        netrjs
finger      79/tcp
www     80/tcp        http        # WorldWideWeb HTTP
www     80/udp                # HyperText Transfer Protocol
link        87/tcp        ttylink
kerberos    88/tcp        kerberos5 krb5 kerberos-sec    # Kerberos v5
kerberos    88/udp        kerberos5 krb5 kerberos-sec    # Kerberos v5
supdup      95/tcp
hostnames   101/tcp        hostname    # usually from sri-nic
iso-tsap    102/tcp        tsap        # part of ISODE
acr-nema    104/tcp        dicom        # Digital Imag. & Comm. 300
acr-nema    104/udp        dicom        # Digital Imag. & Comm. 300
csnet-ns    105/tcp        cso-ns        # also used by CSO name server
csnet-ns    105/udp        cso-ns
rtelnet     107/tcp                # Remote Telnet
rtelnet     107/udp
pop2        109/tcp        postoffice pop-2 # POP version 2
pop2        109/udp        pop-2
pop3        110/tcp        pop-3        # POP version 3
pop3        110/udp        pop-3
sunrpc      111/tcp        portmapper    # RPC 4.0 portmapper
sunrpc      111/udp        portmapper
auth        113/tcp        authentication tap ident
sftp        115/tcp
uucp-path   117/tcp
```

```
nntp        119/tcp        readnews untp    # USENET News Transfer
Protocol
ntp     123/tcp
ntp     123/udp                # Network Time Protocol
pwdgen      129/tcp                # PWDGEN service
pwdgen      129/udp                # PWDGEN service
loc-srv     135/tcp        epmap        # Location Service
loc-srv     135/udp        epmap
netbios-ns  137/tcp                # NETBIOS Name Service
netbios-ns  137/udp
netbios-dgm 138/tcp                # NETBIOS Datagram Service
netbios-dgm 138/udp
netbios-ssn 139/tcp                # NETBIOS session service
netbios-ssn 139/udp
imap2       143/tcp        imap        # Interim Mail Access P 2 and 4
imap2       143/udp        imap
snmp        161/tcp                # Simple Net Mgmt Protocol
snmp        161/udp                # Simple Net Mgmt Protocol
snmp-trap   162/tcp        snmptrap    # Traps for SNMP
snmp-trap   162/udp        snmptrap    # Traps for SNMP
cmip-man    163/tcp                # ISO mgmt over IP (CMOT)
cmip-man    163/udp
cmip-agent  164/tcp
cmip-agent  164/udp
mailq       174/tcp            # Mailer transport queue for Zmailer
mailq       174/udp            # Mailer transport queue for Zmailer
xdmcp       177/tcp                # X Display Mgr. Control Proto
xdmcp       177/udp
nextstep    178/tcp        NeXTStep NextStep    # NeXTStep window
nextstep    178/udp        NeXTStep NextStep    #  server
bgp     179/tcp                # Border Gateway Protocol
bgp     179/udp
prospero    191/tcp                # Cliff Neuman's Prospero
prospero    191/udp
irc     194/tcp                # Internet Relay Chat
irc     194/udp
smux        199/tcp                # SNMP Unix Multiplexer
smux        199/udp
at-rtmp     201/tcp                # AppleTalk routing
at-rtmp     201/udp
at-nbp      202/tcp                # AppleTalk name binding
at-nbp      202/udp
at-echo     204/tcp                # AppleTalk echo
at-echo     204/udp
at-zis      206/tcp                # AppleTalk zone information
at-zis      206/udp
qmtp        209/tcp                # Quick Mail Transfer Protocol
qmtp        209/udp                # Quick Mail Transfer Protocol
z3950       210/tcp        wais        # NISO Z39.50 database
z3950       210/udp        wais
ipx     213/tcp                # IPX
```

```
ipx     213/udp
imap3       220/tcp                 # Interactive Mail Access
imap3       220/udp                 # Protocol v3
pawserv     345/tcp                 # Perf Analysis Workbench
pawserv     345/udp
zserv       346/tcp                 # Zebra server
zserv       346/udp
fatserv     347/tcp                 # Fatmen Server
fatserv     347/udp
rpc2portmap 369/tcp
rpc2portmap 369/udp                 # Coda portmapper
codaauth2   370/tcp
codaauth2   370/udp                 # Coda authentication server
clearcase   371/tcp         Clearcase
clearcase   371/udp         Clearcase
ulistserv   372/tcp                 # UNIX Listserv
ulistserv   372/udp
ldap        389/tcp             # Lightweight Directory Access Protocol
ldap        389/udp
imsp        406/tcp             # Interactive Mail Support Protocol
imsp        406/udp
svrloc      427/tcp                 # Server Location
svrloc      427/udp                 # Server Location
https       443/tcp                 # http protocol over TLS/SSL
https       443/udp
snpp        444/tcp                 # Simple Network Paging Protocol
snpp        444/udp
microsoft-ds    445/tcp                 # Microsoft Naked CIFS
microsoft-ds    445/udp
kpasswd     464/tcp
kpasswd     464/udp
saft        487/tcp             # Simple Asynchronous File Transfer
saft        487/udp
isakmp      500/tcp             # IPsec - Internet Security Association
isakmp      500/udp             #  and Key Management Protocol
rtsp        554/tcp             # Real Time Stream Control Protocol
rtsp        554/udp             # Real Time Stream Control Protocol
nqs     607/tcp                 # Network Queuing system
nqs     607/udp
npmp-local  610/tcp         dqs313_qmaster        # npmp-local / DQS
npmp-local  610/udp         dqs313_qmaster
npmp-gui    611/tcp         dqs313_execd        # npmp-gui / DQS
npmp-gui    611/udp         dqs313_execd
hmmp-ind    612/tcp         dqs313_intercell    # HMMP Indication / DQS
hmmp-ind    612/udp         dqs313_intercell
qmqp        628/tcp
qmqp        628/udp
ipp     631/tcp                 # Internet Printing Protocol
ipp     631/udp
#
# UNIX specific services
```

```
#
exec        512/tcp
biff        512/udp        comsat
login       513/tcp
who     513/udp        whod
shell       514/tcp        cmd        # no passwords used
syslog      514/udp
printer     515/tcp        spooler        # line printer spooler
talk        517/udp
ntalk       518/udp
route       520/udp        router routed    # RIP
timed       525/udp        timeserver
tempo       526/tcp        newdate
courier     530/tcp        rpc
conference  531/tcp        chat
netnews     532/tcp        readnews
netwall     533/udp                # for emergency broadcasts
gdomap      538/tcp                # GNUstep distributed objects
gdomap      538/udp
uucp        540/tcp        uucpd        # uucp daemon
klogin      543/tcp                # Kerberized `rlogin' (v5)
kshell      544/tcp        krcmd        # Kerberized `rsh' (v5)
dhcpv6-client   546/tcp
dhcpv6-client   546/udp
dhcpv6-server   547/tcp
dhcpv6-server   547/udp
afpovertcp  548/tcp                # AFP over TCP
afpovertcp  548/udp
idfp        549/tcp
idfp        549/udp
remotefs    556/tcp        rfs_server rfs    # Brunhoff remote
filesystem
nntps       563/tcp        snntp        # NNTP over SSL
nntps       563/udp        snntp
submission  587/tcp                # Submission [RFC4409]
submission  587/udp
ldaps       636/tcp                # LDAP over SSL
ldaps       636/udp
tinc        655/tcp                # tinc control port
tinc        655/udp
silc        706/tcp
silc        706/udp
kerberos-adm    749/tcp                # Kerberos `kadmin' (v5)
#
webster     765/tcp                # Network dictionary
webster     765/udp
rsync       873/tcp
rsync       873/udp
ftps-data   989/tcp                # FTP over SSL (data)
ftps        990/tcp
telnets     992/tcp                # Telnet over SSL
```

```
telnets     992/udp
imaps       993/tcp                # IMAP over SSL
imaps       993/udp
ircs        994/tcp                # IRC over SSL
ircs        994/udp
pop3s       995/tcp                # POP-3 over SSL
pop3s       995/udp
#
# From ``Assigned Numbers'':
#
#> The Registered Ports are not controlled by the IANA and on most
systems
#> can be used by ordinary user processes or programs executed by
ordinary
#> users.
#
#> Ports are used in the TCP [45,106] to name the ends of logical
#> connections which carry long term conversations.  For the purpose of
#> providing services to unknown callers, a service contact port is
#> defined.  This list specifies the port used by the server process as
its
#> contact port.  While the IANA can not control uses of these ports it
#> does register or list uses of these ports as a convienence to the
#> community.
#
socks       1080/tcp            # socks proxy server
socks       1080/udp
proofd      1093/tcp
proofd      1093/udp
rootd       1094/tcp
rootd       1094/udp
openvpn     1194/tcp
openvpn     1194/udp
rmiregistry 1099/tcp            # Java RMI Registry
rmiregistry 1099/udp
kazaa       1214/tcp
kazaa       1214/udp
nessus      1241/tcp            # Nessus vulnerability
nessus      1241/udp            #  assessment scanner
lotusnote   1352/tcp    lotusnotes    # Lotus Note
lotusnote   1352/udp    lotusnotes
ms-sql-s    1433/tcp            # Microsoft SQL Server
ms-sql-s    1433/udp
ms-sql-m    1434/tcp            # Microsoft SQL Monitor
ms-sql-m    1434/udp
ingreslock  1524/tcp
ingreslock  1524/udp
prospero-np 1525/tcp            # Prospero non-privileged
prospero-np 1525/udp
datametrics 1645/tcp    old-radius
datametrics 1645/udp    old-radius
```

```
sa-msg-port 1646/tcp    old-radacct
sa-msg-port 1646/udp    old-radacct
kermit      1649/tcp
kermit      1649/udp
l2f     1701/tcp    l2tp
l2f     1701/udp    l2tp
radius      1812/tcp
radius      1812/udp
radius-acct 1813/tcp    radacct        # Radius Accounting
radius-acct 1813/udp    radacct
msnp        1863/tcp            # MSN Messenger
msnp        1863/udp
unix-status 1957/tcp            # remstats unix-status server
log-server  1958/tcp            # remstats log server
remoteping  1959/tcp            # remstats remoteping server
cisco-sccp  2000/tcp            # Cisco SCCP
cisco-sccp  2000/udp
search      2010/tcp    ndtp
pipe_server 2010/tcp
nfs     2049/tcp            # Network File System
nfs     2049/udp            # Network File System
gnunet      2086/tcp
gnunet      2086/udp
rtcm-sc104  2101/tcp            # RTCM SC-104 IANA 1/29/99
rtcm-sc104  2101/udp
gsigatekeeper   2119/tcp
gsigatekeeper   2119/udp
gris        2135/tcp        # Grid Resource Information Server
gris        2135/udp        # Grid Resource Information Server
cvspserver  2401/tcp            # CVS client/server operations
cvspserver  2401/udp
venus       2430/tcp            # codacon port
venus       2430/udp            # Venus callback/wbc interface
venus-se    2431/tcp            # tcp side effects
venus-se    2431/udp            # udp sftp side effect
codasrv     2432/tcp            # not used
codasrv     2432/udp            # server port
codasrv-se  2433/tcp            # tcp side effects
codasrv-se  2433/udp            # udp sftp side effect
mon     2583/tcp            # MON traps
mon     2583/udp
dict        2628/tcp            # Dictionary server
dict        2628/udp
gsiftp      2811/tcp
gsiftp      2811/udp
gpsd        2947/tcp
gpsd        2947/udp
gds_db      3050/tcp            # InterBase server
gds_db      3050/udp
icpv2       3130/tcp    icp        # Internet Cache Protocol
icpv2       3130/udp    icp
```

```
mysql       3306/tcp
mysql       3306/udp
nut     3493/tcp            # Network UPS Tools
nut     3493/udp
distcc      3632/tcp            # distributed compiler
distcc      3632/udp
daap        3689/tcp            # Digital Audio Access Protocol
daap        3689/udp
svn     3690/tcp    subversion    # Subversion protocol
svn     3690/udp    subversion
suucp       4031/tcp            # UUCP over SSL
suucp       4031/udp            # UUCP over SSL
sysrqd      4094/tcp            # sysrq daemon
sysrqd      4094/udp            # sysrq daemon
sieve       4190/tcp            # ManageSieve Protocol
epmd        4369/tcp            # Erlang Port Mapper Daemon
epmd        4369/udp            # Erlang Port Mapper Daemon
remctl      4373/tcp        # Remote Authenticated Command Service
remctl      4373/udp        # Remote Authenticated Command Service
iax     4569/tcp            # Inter-Asterisk eXchange
iax     4569/udp
mtn     4691/tcp            # monotone Netsync Protocol
mtn     4691/udp            # monotone Netsync Protocol
radmin-port 4899/tcp            # RAdmin Port
radmin-port 4899/udp
rfe     5002/udp            # Radio Free Ethernet
rfe     5002/tcp
mmcc        5050/tcp    # multimedia conference control tool (Yahoo IM)
mmcc        5050/udp
sip     5060/tcp            # Session Initiation Protocol
sip     5060/udp
sip-tls     5061/tcp
sip-tls     5061/udp
aol     5190/tcp            # AIM
aol     5190/udp
xmpp-client 5222/tcp    jabber-client    # Jabber Client Connection
xmpp-client 5222/udp    jabber-client
xmpp-server 5269/tcp    jabber-server    # Jabber Server Connection
xmpp-server 5269/udp    jabber-server
cfengine    5308/tcp
cfengine    5308/udp
mdns        5353/tcp            # Multicast DNS
mdns        5353/udp            # Multicast DNS
postgresql  5432/tcp    postgres    # PostgreSQL Database
postgresql  5432/udp    postgres
freeciv     5556/tcp    rptp        # Freeciv gameplay
freeciv     5556/udp
amqp        5672/tcp
amqp        5672/udp
amqp        5672/sctp
ggz     5688/tcp            # GGZ Gaming Zone
```

```
ggz     5688/udp            # GGZ Gaming Zone
x11     6000/tcp    x11-0        # X Window System
x11     6000/udp    x11-0
x11-1       6001/tcp
x11-1       6001/udp
x11-2       6002/tcp
x11-2       6002/udp
x11-3       6003/tcp
x11-3       6003/udp
x11-4       6004/tcp
x11-4       6004/udp
x11-5       6005/tcp
x11-5       6005/udp
x11-6       6006/tcp
x11-6       6006/udp
x11-7       6007/tcp
x11-7       6007/udp
gnutella-svc    6346/tcp            # gnutella
gnutella-svc    6346/udp
gnutella-rtr    6347/tcp            # gnutella
gnutella-rtr    6347/udp
sge_qmaster 6444/tcp            # Grid Engine Qmaster Service
sge_qmaster 6444/udp            # Grid Engine Qmaster Service
sge_execd   6445/tcp            # Grid Engine Execution Service
sge_execd   6445/udp            # Grid Engine Execution Service
mysql-proxy 6446/tcp            # MySQL Proxy
mysql-proxy 6446/udp            # MySQL Proxy
afs3-fileserver 7000/tcp    bbs        # file server itself
afs3-fileserver 7000/udp    bbs
afs3-callback   7001/tcp            # callbacks to cache managers
afs3-callback   7001/udp
afs3-prserver   7002/tcp            # users & groups database
afs3-prserver   7002/udp
afs3-vlserver   7003/tcp            # volume location database
afs3-vlserver   7003/udp
afs3-kaserver   7004/tcp            # AFS/Kerberos authentication
afs3-kaserver   7004/udp
afs3-volser 7005/tcp            # volume managment server
afs3-volser 7005/udp
afs3-errors 7006/tcp            # error interpretation service
afs3-errors 7006/udp
afs3-bos    7007/tcp            # basic overseer process
afs3-bos    7007/udp
afs3-update 7008/tcp            # server-to-server updater
afs3-update 7008/udp
afs3-rmtsys 7009/tcp            # remote cache manager service
afs3-rmtsys 7009/udp
font-service    7100/tcp    xfs        # X Font Service
font-service    7100/udp    xfs
http-alt    8080/tcp    webcache    # WWW caching service
http-alt    8080/udp            # WWW caching service
```

```
bacula-dir  9101/tcp            # Bacula Director
bacula-dir  9101/udp
bacula-fd   9102/tcp            # Bacula File Daemon
bacula-fd   9102/udp
bacula-sd   9103/tcp            # Bacula Storage Daemon
bacula-sd   9103/udp
xmms2       9667/tcp    # Cross-platform Music Multiplexing System
xmms2       9667/udp    # Cross-platform Music Multiplexing System
nbd     10809/tcp            # Linux Network Block Device
zabbix-agent    10050/tcp            # Zabbix Agent
zabbix-agent    10050/udp            # Zabbix Agent
zabbix-trapper  10051/tcp            # Zabbix Trapper
zabbix-trapper  10051/udp            # Zabbix Trapper
amanda      10080/tcp            # amanda backup services
amanda      10080/udp
hkp     11371/tcp            # OpenPGP HTTP Keyserver
hkp     11371/udp            # OpenPGP HTTP Keyserver
bprd        13720/tcp            # VERITAS NetBackup
bprd        13720/udp
bpdbm       13721/tcp            # VERITAS NetBackup
bpdbm       13721/udp
bpjava-msvc 13722/tcp            # BP Java MSVC Protocol
bpjava-msvc 13722/udp
vnetd       13724/tcp            # Veritas Network Utility
vnetd       13724/udp
bpcd        13782/tcp            # VERITAS NetBackup
bpcd        13782/udp
vopied      13783/tcp            # VERITAS NetBackup
vopied      13783/udp
dcap        22125/tcp            # dCache Access Protocol
gsidcap     22128/tcp            # GSI dCache Access Protocol
wnn6        22273/tcp            # wnn6
wnn6        22273/udp

#
# Datagram Delivery Protocol services
#
rtmp        1/ddp            # Routing Table Maintenance Protocol
nbp     2/ddp            # Name Binding Protocol
echo        4/ddp            # AppleTalk Echo Protocol
zip     6/ddp            # Zone Information Protocol

#=====================================================================
===
# The remaining port numbers are not as allocated by IANA.
#=====================================================================
===

# Kerberos (Project Athena/MIT) services
# Note that these are for Kerberos v4, and are unofficial.  Sites
running
```

```
# v4 should uncomment these and comment out the v5 entries above.
#
kerberos4   750/udp        kerberos-iv kdc    # Kerberos (server)
kerberos4   750/tcp        kerberos-iv kdc
kerberos_master 751/udp               # Kerberos authentication
kerberos_master 751/tcp
passwd_server   752/udp               # Kerberos passwd server
krb_prop    754/tcp        krb5_prop hprop    # Kerberos slave
propagation
krbupdate   760/tcp        kreg        # Kerberos registration
swat        901/tcp                # swat
kpop        1109/tcp           # Pop with Kerberos
knetd       2053/tcp           # Kerberos de-multiplexor
zephyr-srv  2102/udp           # Zephyr server
zephyr-clt  2103/udp           # Zephyr serv-hm connection
zephyr-hm   2104/udp           # Zephyr hostmanager
eklogin     2105/tcp           # Kerberos encrypted rlogin
# Hmmm. Are we using Kv4 or Kv5 now? Worrying.
# The following is probably Kerberos v5  --- ajt@debian.org
(11/02/2000)
kx      2111/tcp           # X over Kerberos
iprop       2121/tcp           # incremental propagation
#
# Unofficial but necessary (for NetBSD) services
#
supfilesrv  871/tcp                # SUP server
supfiledbg  1127/tcp           # SUP debugging

#
# Services added for the Debian GNU/Linux distribution
#
linuxconf   98/tcp                # LinuxConf
poppassd    106/tcp                # Eudora
poppassd    106/udp
ssmtp       465/tcp        smtps        # SMTP over SSL
moira_db    775/tcp                # Moira database
moira_update    777/tcp                # Moira update protocol
moira_ureg  779/udp                # Moira user registration
spamd       783/tcp                # spamassassin daemon
omirr       808/tcp        omirrd        # online mirror
omirr       808/udp        omirrd
customs     1001/tcp           # pmake customs server
customs     1001/udp
skkserv     1178/tcp           # skk jisho server port
predict     1210/udp           # predict -- satellite tracking
rmtcfg      1236/tcp           # Gracilis Packeten remote config
server
wipld       1300/tcp           # Wipl network monitor
xtel        1313/tcp           # french minitel
xtelw       1314/tcp           # french minitel
support     1529/tcp           # GNATS
```

```
cfinger     2003/tcp            # GNU Finger
frox        2121/tcp            # frox: caching ftp proxy
ninstall    2150/tcp            # ninstall service
ninstall    2150/udp
zebrasrv    2600/tcp            # zebra service
zebra       2601/tcp            # zebra vty
ripd        2602/tcp            # ripd vty (zebra)
ripngd      2603/tcp            # ripngd vty (zebra)
ospfd       2604/tcp            # ospfd vty (zebra)
bgpd        2605/tcp            # bgpd vty (zebra)
ospf6d      2606/tcp            # ospf6d vty (zebra)
ospfapi     2607/tcp            # OSPF-API
isisd       2608/tcp            # ISISd vty (zebra)
afbackup    2988/tcp            # Afbackup system
afbackup    2988/udp
afmbackup   2989/tcp            # Afmbackup system
afmbackup   2989/udp
xtell       4224/tcp            # xtell server
fax     4557/tcp            # FAX transmission service (old)
hylafax     4559/tcp            # HylaFAX client-server protocol (new)
distmp3     4600/tcp            # distmp3host daemon
munin       4949/tcp    lrrd        # Munin
enbd-cstatd 5051/tcp            # ENBD client statd
enbd-sstatd 5052/tcp            # ENBD server statd
pcrd        5151/tcp            # PCR-1000 Daemon
noclog      5354/tcp            # noclogd with TCP (nocol)
noclog      5354/udp            # noclogd with UDP (nocol)
hostmon     5355/tcp            # hostmon uses TCP (nocol)
hostmon     5355/udp            # hostmon uses UDP (nocol)
rplay       5555/udp            # RPlay audio service
nrpe        5666/tcp            # Nagios Remote Plugin Executor
nsca        5667/tcp            # Nagios Agent - NSCA
mrtd        5674/tcp            # MRT Routing Daemon
bgpsim      5675/tcp            # MRT Routing Simulator
canna       5680/tcp            # cannaserver
sane-port   6566/tcp    sane saned    # SANE network scanner daemon
ircd        6667/tcp            # Internet Relay Chat
zope-ftp    8021/tcp            # zope management by ftp
tproxy      8081/tcp            # Transparent Proxy
omniorb     8088/tcp            # OmniORB
omniorb     8088/udp
clc-build-daemon 8990/tcp           # Common lisp build daemon
xinetd      9098/tcp
mandelspawn 9359/udp    mandelbrot    # network mandelbrot
git     9418/tcp            # Git Version Control System
zope        9673/tcp            # zope server
webmin      10000/tcp
kamanda     10081/tcp            # amanda backup services (Kerberos)
kamanda     10081/udp
amandaidx   10082/tcp            # amanda backup services
amidxtape   10083/tcp            # amanda backup services
```

```
smsqp       11201/tcp            # Alamin SMS gateway
smsqp       11201/udp
xpilot      15345/tcp            # XPilot Contact Port
xpilot      15345/udp
sgi-cmsd    17001/udp        # Cluster membership services daemon
sgi-crsd    17002/udp
sgi-gcd     17003/udp            # SGI Group membership daemon
sgi-cad     17004/tcp            # Cluster Admin daemon
isdnlog     20011/tcp            # isdn logging system
isdnlog     20011/udp
vboxd       20012/tcp            # voice box system
vboxd       20012/udp
binkp       24554/tcp            # binkp fidonet protocol
asp     27374/tcp            # Address Search Protocol
asp     27374/udp
csync2      30865/tcp            # cluster synchronization tool
dircproxy   57000/tcp            # Detachable IRC Proxy
tfido       60177/tcp            # fidonet EMSI over telnet
fido        60179/tcp            # fidonet EMSI over TCP

# Local services
```

Sources de cette documentation

- http://www.humbug.in/docs/ubuntu-server-guide-fr-10.04/firewall.html#firewall-ufw - **Lien Obsolète**
- http://dl.dropbox.com/u/483488/references/secure_server.html
- http://mauroandres.wordpress.com/2009/12/14/build-a-secure-desktop-firewall-with-ufw-part-i/ (En anglais mais exemples compréhensibles)
- http://mauroandres.wordpress.com/2010/01/28/build-a-secure-desktop-firewall-with-ufw-part-ii/ (En anglais mais exemples compréhensibles)
- http://doc.ubuntu-fr.org/ufw

Liens

- ufw en graphique : ufw en graphique (xfce).

[1)]
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:
http://debian-facile.org/ - **Documentation - Wiki**

Permanent link:
http://debian-facile.org/doc:systeme:ufw

Last update: **26/06/2018 17:51**