HOWTO: The Ubuntu firewall ufw

Introduction

Distributions like Ubuntu, have a built-in firewall that bears the name ufw (uncomplicated firewall). With the firewall ufw, Ubuntu facilitates the complicated fiddling with netfilter / iptables. The user does not need to strive the package manager like apt-get or aptitude to install. ufw is already installed, but it must be enabled and configured on the Linux shell or the GUI (Gufw). The activation of Ubuntu ufw firewall is recommended, in the case when the protection of a computer must be guaranteed not only against intruders from the internet, but also from the internal network, eg, for growing business networks. A firewall, such as Ubuntu ufw, does not provide the ultimate protection against all dangers. But it is a “check” on a list, which must necessarily belong to the basic safety concept of a Linux system, if it is to be considered as cured.

When you turn on the firewall ufw, it already uses some pre-configured rules of Ubuntu. To not be excluded in the following configuration of the computer itself, it is recommended to physically sit in front of the PC to which one is operating. In this paper, only the configuration of the Ubuntu firewall ufw, from the Linux shell is given attention.

Switching on and off

The following commands set the Ubuntu ufw firewall turned on or off:

```
sudo ufw enable
Firewall is active and enabled on system startup

sudo ufw disable
Firewall stopped and disabled on system startup
```

Status output

The status of the Ubuntu firewall ufw can be displayed by three different commands. Which command is used is up to one self:

```
sudo ufw status
Status: active
```

or

```
sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip
```

or

```
sudo ufw status numbered
Status: active

To                         Action      From
--                         ------      ----
[ 1] 22/tcp on eth0        ALLOW IN    172.17.0.1
[ 2] 443 on eth0           ALLOW IN    Anywhere
[ 3] 80 on eth0            ALLOW IN    Anywhere
```

Reports

To see which ports can be unlocked, a report from the Ubuntu firewall ufw can be displayed:

```
sudo ufw show LISTENING
tcp:
22 * (sshd)
443 * (apache2)
80 * (apache2)
udp:
68 * (dhclient)
```

To all port entries in the above example, no rules are assigned in the Ubuntu firewall. Unlike here:

```
sudo ufw show LISTENING
tcp:
22 * (sshd)
[ 1] allow in on eth0 from 172.17.0.1 to any port 22 proto tcp

443 * (apache2)
[ 2] allow in on eth0 to any port 443

80 * (apache2)
[ 3] allow in on eth0 to any port 80
```

```
udp:
68 * (dhclient)
```

Firewall rules

allow

There is not only is one notation in the Ubuntu firewall ufw to define a rule. The shortest form, however, is the following:

```
sudo ufw allow in PORT[/Protokoll]
```

Examples:
Accepts incoming TCP and UDP packets, only TCP packets and UDP packets on port 80:

```
sudo ufw allow in 80
sudo ufw allow in 80/tcp
sudo ufw allow in 80/udp
```

But preferred is a slightly more detailed notation for rule creation:

```
sudo ufw allow in [on INTERFACE] [from ADDRESS [port PORT]] [to
ADDRESS [port PORT]] [proto protocol]
```

Examples:
Accepts incoming packets on the network interface eth0 from any address on its own port 80 with TCP and UDP packets, only TCP packets and UDP packets:

```
sudo ufw allow in on eth0 from any to any port 80
sudo ufw allow in on eth0 from any to any port 80 proto tcp
sudo ufw allow in on eth0 from any to any port 80 proto udp
```

Accepts incoming packets on the network interface eth0 from the address 172.17.0.1, to its own port 443 with TCP and UDP packets, only TCP packets and UDP packets:

```
sudo ufw allow in on eth0 from 172.17.0.1 to any port 443
sudo ufw allow in on eth0 from 172.17.0.1 to any port 443 proto tcp
sudo ufw allow in on eth0 from 172.17.0.1 to any port 443 proto udp
```

Or with an indication of the network and subnet mask:

```
sudo ufw allow in on eth0 from 172.17.0.0/8 to any port 443
sudo ufw allow in on eth0 from 172.17.0.0/16 to any port 443 proto
tcp
```

```
sudo ufw allow in on eth0 from 172.17.0.0/24 to any port 443 proto
udp
```

deny

The spelling of deny rules in the firewall ufw of Ubuntu, is just like with allow. It is used eg, to block the access to a service from a computer or a network segment:

```
sudo ufw deny in on eth0 from 172.17.0.1 to any port 22
sudo ufw deny in on eth0 from 172.17.0.0/16 to any port 22
```

Allow and deny rules together

Allow and deny rules can be used in any case in ufw together. Here, it is shown how the access from two different computers is completely blocked, while the network 172.17.0.0/24 is allowed:

```
sudo ufw deny in on eth0 from 172.17.0.1 to any port 22
sudo ufw deny in on eth0 from 172.17.0.2 to any port 22
sudo ufw allow in on eth0 from 172.17.0.0/24 to any port 22 proto
tcp
```

Delete rules

In order to delete an created rule in the Ubuntu firewall, just a delete is prepended to the allow command:

```
sudo ufw delete allow in on eth0 from any to any port 80
sudo ufw delete allow in on eth0 from any to any port 80 proto tcp
sudo ufw delete allow in on eth0 from any to any port 80 proto udp
```

It’s even easier to operate, if the number of the rule is entered. The number can be displayed with the command *ufw show LISTENING*:

```
sudo ufw show LISTENING
tcp:
22 * (sshd)
[ 1] allow in on eth0 from 172.17.0.1 to any port 22 proto tcp

443 * (apache2)
[ 2] allow in on eth0 to any port 443

80 * (apache2)
[ 3] allow in on eth0 to any port 80
```

```
udp:
68 * (dhclient)
```

The rule with the number 3 is deleted like this:

```
sudo ufw delete 3
sudo ufw show LISTENING
tcp:
22 * (sshd)
[ 1] allow in on eth0 from 172.17.0.1 to any port 22 proto tcp

443 * (apache2)
[ 2] allow in on eth0 to any port 443

80 * (apache2)
udp:
68 * (dhclient)
```

Others

block ping

In the default configuration, ufw allows the ping of your own computer. It helps in the basic network problem analysis. If you want to disable the rules in the Ubuntu firewall ufw, you need to edit the */etc/ufw/before.rules* file. The following lines must be either commented out or changed from “ACCEPT” to “DROP”:

```
# ok icmp codes
#-A ufw-before-input -p icmp --icmp-type destination-unreachable -j
ACCEPT
#-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type parameter-problem -j
ACCEPT
#-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp codes
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j
DROP
-A ufw-before-input -p icmp --icmp-type source-quench -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

DHCP client

The standard way to assign IP addresses is via DHCP. The pre-configured rules allow therefore to do it. If one prefer to manually assign the computer a static IP address, so he can uncomment this rule also.

```
# allow dhcp client to work
#-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT
```

Logging

Logging can be turned on using the following commands and adjusted to the desired level.

```
sudo ufw logging off
sudo ufw logging on
sudo ufw logging low | medium | high | full
```

By default, it is logged in the file */var/log/ufw.log*. Each setting over medium can make the log file to rise sharply.

Well Known Ports

There are more than a handful of firewall ports that must a SOHO user know, if he runs or want to run a firewall. The following are some of the so-called *Well Known Ports* which are listed in a table. The specified ports are standardized, that is, they meet not only to the Ubuntu firewall ufw:

Well Known Ports

Port	Protokoll	Name in /ets/services	Beschreibung
21	tcp	ftp	File Transmission Protokoll
22	tcp, udp	ssh	Secure Shell Remote-Login Protokoll
25	tcp	smtp	Mailserver – Email-Versand
53	tcp, udp	domain	Domain Name System
80	tcp	http	HTTP-Protocol to surf the World Wide Web
110	tcp	pop3	POP Version 3

143	tcp, udp	imap2	IMAP4 – Internet Message Access Protocol
389	tcp, udp	ldap	LDAP – Lightweight Directory Access Protocol
443	tcp	https	HTTP-Protokoll but via TLS/SSL – HTTPS
993	tcp	imaps	IMAP4 via SSL – IMAPS
995	tcp	pop3s	POP Version 3 via SSL – POP3S
1194	tcp, udp	openvpn	OpenVPN – Vitual Private Network

Conclusion

For users, who simply want to have protected their computer by a firewall, the preconfigured Ubuntu rules should be more or less sufficient. In addition, to the switching of ufw, nothing else is to do further for them. To configure a firewall for offering a service computer, some care is needed. Catch best viewed only with the *allow* rules in the more detailed notation. First test the services to access the various programs, eg, with nmap as the analysis tool. To verify that you have not drilled more holes in the firewall as intended.

External Links

http://manpages.ubuntu.com/manpages/lucid/man8/ufw.8.html
https://help.ubuntu.com/community/UFW