Installation and Configuration of Uncomplicated Firewall (UFW) on Ubuntu Server

Eliyah Watson

3/10/2025

Installation of UFW on Ubuntu Server

First, we need to install UFW and its packages by navigating to the terminal and input:

$ sudo apt install ufw

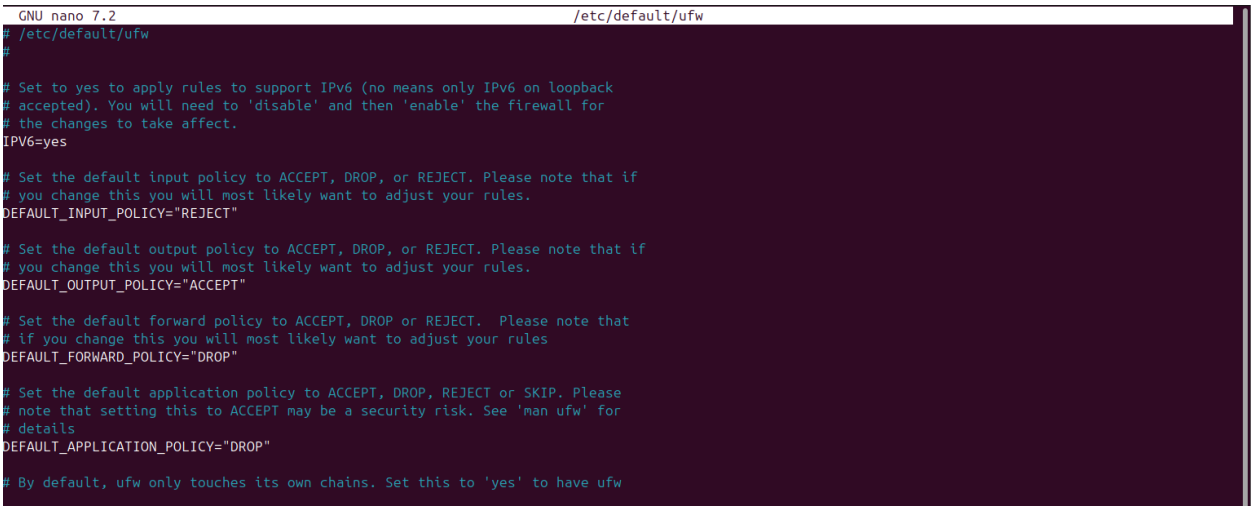
```
vsoc@vsoc:/etc/ansible/elk-ansible$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
  acpi-support acpid aisleriot apturl apturl-common branding-ubuntu
  cheese cheese-common cpp-11 endeavour endeavour-common fonts-beng
  fonts-beng-extra fonts-deva fonts-deva-extra fonts-gargi
  fonts-gubbi fonts-gujr fonts-gujr-extra fonts-guru fonts-guru-extra
  fonts-indic fonts-kacst fonts-kacst-one fonts-kalapi
  fonts-khmeros-core fonts-knda fonts-lao fonts-liberation2
  fonts-lklug-sinhala fonts-lohit-beng-assamese
  fonts-lohit-beng-bengali fonts-lohit-deva fonts-lohit-gujr
  fonts-lohit-guru fonts-lohit-knda fonts-lohit-mlym fonts-lohit-orya
  fonts-lohit-taml fonts-lohit-taml-classical fonts-lohit-telu
  fonts-mlym fonts-nakula fonts-navilu fonts-orya fonts-orya-extra
  fonts-pagul fonts-sahadeva fonts-samyak-deva fonts-samyak-gujr
  fonts-samyak-mlym fonts-samyak-taml fonts-sarai
  fonts-sil-abyssinica fonts-sil-annapurna fonts-sil-padauk fonts-smc
  fonts-smc-anjalioldlipi fonts-smc-chilanka fonts-smc-dyuthi
  fonts-smc-gayathri fonts-smc-karumbi fonts-smc-keraleeyam
  fonts-smc-manjari fonts-smc-meera fonts-smc-rachana
  fonts-smc-raghumalayalamsans fonts-smc-suruma fonts-smc-uroob
  fonts-taml fonts-telu fonts-telu-extra fonts-teluguvijayam
  fonts-thai-tlwg fonts-tibetan-machine fonts-tlwg-garuda
  fonts-tlwg-garuda-ttf fonts-tlwg-kinnari fonts-tlwg-kinnari-ttf
  fonts-tlwg-laksaman fonts-tlwg-laksaman-ttf fonts-tlwg-loma
  fonts-tlwg-loma-ttf fonts-tlwg-mono fonts-tlwg-mono-ttf
  fonts-tlwg-norasi fonts-tlwg-norasi-ttf fonts-tlwg-purisa
```

Configuration of UFW on Ubuntu Server

The first thing you want to do is set up your UFW before enabling it, because enabling it before any configuration takes place may cause you to be locked out of your virtual machine.

To configure the default network traffic policies on UFW, open the editor of the policy document:
$ sudo nano /etc/default/ufw

Modify the following settings:
IPV6=yes
DEFAULT_INPUT_POLICY=“DENY”
DEFAULT_OUTPUT_POLICY=“ACCEPT”
DEFAULT_FORWARD_POLICY=“DROP”
DEFAULT_APPLICATION_POLICY=“DROP”



These settings have the following meanings:

1. UFW will be handling IPv4 as well as IPv6 traffic and apply the configured rules to both
2. If incoming network traffic matches none of the specified rules in the configuration, it is implicitly denied, unless there are rules that allow the traffic.
3. By default, outcoming network traffic from your system should be implicitly allowed
4. If forwarded network traffic matches none of the specified rules in the configuration, it is silently dropped, unless there are rules that allow the traffic.
5. By default, all applications are blocked by default unless there are rules that allow the applications to use the network

Rule definitions for essential protocols/SOC applications

We need to configure firewall rules while performing hardening for the most important protocols and the SOC applications:

$ sudo ufw allow from [VM IP] to any port 22 proto tcp
$ sudo ufw allow from [VM IP] to any port 80 proto tcp
$ sudo ufw allow from [VM IP] to any port 443 proto tcp
$ sudo ufw allow from [VM IP] to any port 9200 proto tcp
$ sudo ufw allow from [VM IP] to any port 5000 proto tcp
$ sudo ufw allow from [VM IP] to any port 5601 proto tcp
$ sudo ufw allow from [VM IP] to any port 514 proto tcp
$ sudo ufw allow from [VM IP] to any port 514 proto udp
$ sudo ufw allow from [VM IP] to any port 21 proto tcp
$ sudo ufw allow from [VM IP] to any port 53 proto tcp
$ sudo ufw allow from [VM IP] to any port 53 proto udp
$ sudo ufw allow from [VM IP] to any port 25 proto tcp
$ sudo ufw allow from [VM IP] to any port 24224 proto tcp
$ sudo ufw allow from [VM IP] to any port 24224 proto udp

$ sudo ufw allow from [VM IP] to any port 161 proto udp
$ sudo ufw allow from [VM IP] to any port 8888 proto tcp
$ sudo ufw allow from [VM IP] to any port 3000 proto tcp

The following rules state:

- To allow SSH traffic on port 22 from the VM's IP address
- To allow HTTP traffic on port 80 from the VM's IP address
- To allow HTTPS traffic on port 443 from the VM's IP address
- To allow TCP traffic on port 9200 and 9300, the default ports for Elasticsearch's REST API, from the VM's IP address
- To allow TCP traffic on port 5000, the default port for Logstash to receive raw data for log ingestion, from the VM's IP address
- To allow TCP traffic on port 5601, the default port for Kibana (used for the web interface), from the VM's IP address
- To allow UDP traffic on port 514, the default port for Snort to forward logs to Syslog-ng, from the VM's IP address
- To allow TCP traffic on port 21 (FTP traffic monitoring), from the VM's IP address
- To allow TCP and UDP traffic on port 53 (DNS monitoring), from the VM's IP address
- To allow TCP traffic on port 25 (SMTP monitoring or email monitoring), from the VM's IP address
- To allow TCP and UDP traffic on port 24224, the default port for Fluentd to receive logs securely and when speed is more important than the priority of receiving logs, from the VM's IP address
- To allow TCP traffic on port 514, because Snort uses 514 already and Syslog-ng can also use it for TCP connections, from the VM's IP address
- To allow UDP traffic on port 161 for Nagios to receive SNMP data from network devices for monitoring, from the VM's IP address
- To allow TCP traffic on port 3000, the default port to allow access to the Grafana web interface, from the VM's IP address
- To allow TCP traffic on port 8888, the default port for accessing MITRE Caldera's web interface, from the VM's IP address

Result

The results of the firewall rules in a list format are shown by:
$ sudo ufw status

```
vsoc@vsoc:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       192.168.234.128
80/tcp                     ALLOW       192.168.234.128
443/tcp                    ALLOW       192.168.234.128
9200/tcp                   ALLOW       192.168.234.128
5000/tcp                   ALLOW       192.168.234.128
5601/tcp                   ALLOW       192.168.234.128
514/udp                    ALLOW       192.168.234.128
514/tcp                    ALLOW       192.168.234.128
21/tcp                     ALLOW       192.168.234.128
53/tcp                     ALLOW       192.168.234.128
53/udp                     ALLOW       192.168.234.128
25/tcp                     ALLOW       192.168.234.128
24224/tcp                  ALLOW       192.168.234.128
24224/udp                  ALLOW       192.168.234.128
161/udp                    ALLOW       192.168.234.128
8888/tcp                   ALLOW       192.168.234.128
3000/tcp                   ALLOW       192.168.234.128

vsoc@vsoc:~$
```

If you want a numbered list:

$ sudo ufw status numbered

```
vsoc@vsoc:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    192.168.234.128
[ 2] 80/tcp                     ALLOW IN    192.168.234.128
[ 3] 443/tcp                    ALLOW IN    192.168.234.128
[ 4] 9200/tcp                   ALLOW IN    192.168.234.128
[ 5] 5000/tcp                   ALLOW IN    192.168.234.128
[ 6] 5601/tcp                   ALLOW IN    192.168.234.128
[ 7] 514/udp                    ALLOW IN    192.168.234.128
[ 8] 514/tcp                    ALLOW IN    192.168.234.128
[ 9] 21/tcp                     ALLOW IN    192.168.234.128
[10] 53/tcp                     ALLOW IN    192.168.234.128
[11] 53/udp                     ALLOW IN    192.168.234.128
[12] 25/tcp                     ALLOW IN    192.168.234.128
[13] 24224/tcp                  ALLOW IN    192.168.234.128
[14] 24224/udp                  ALLOW IN    192.168.234.128
[15] 161/udp                    ALLOW IN    192.168.234.128
[16] 8888/tcp                   ALLOW IN    192.168.234.128
[17] 3000/tcp                   ALLOW IN    192.168.234.128

vsoc@vsoc:~$
```