**Linux Uncomplicated Firewall & iptables Basics**

**Troubleshooting:**

**1. Check UFW status, enable if necessary**

* + ufw status
  + ufw enable

**2. Get UFW Info**

* + grep 'DEFAULT\_' /etc/default/ufw
  + ufw app list
  + ufw app info <profile>
  + ufw app default ALLOW
  + ufw app update
  + ufw app update --add-new <profile>

**3. Ensure logging is enabled**

* + sudo ufw logging on

**4. If a singular service doesn’t work**

* + ufw allow|deny service|port

OR

* + ufw allow|deny [proto <protocol>] [from <address> [port <port>]] [to <address> [port <port>]]

**5. Manage incoming and outcoming traffic**

* + sudo ufw deny from 15.15.15.51
  + sudo ufw deny in on eth0 from 15.15.15.51

**6. Confirm mirroring on ports**  
 More research needed

**Common Services:**

SSH - 22

HTTP - 80

HTTPS - 443

MySQL - 3306

PostgreSQL - 5432

SMTP - 25, 587 outbound

IMAP - 143

IMAPS - 993

POP3 - 110

POP3S - 995

**Useful file paths:**

**/etc/default/ufw**: high level configuration, such as default policies, IPv6 support and kernel modules to use

**/etc/ufw/before[6].rules**: rules in these files are evaluated before any rules added via the ufw command

**/etc/ufw/after[6].rules**: rules in these files are evaluated after any rules added via the ufw command

**/etc/ufw/sysctl.conf**: kernel network tunables

**/var/lib/ufw/user[6].rules** or **/lib/ufw/user[6].rules** (0.28 and later): rules added via the ufw command (should not normally be edited by hand)

**/etc/ufw/ufw.conf**: sets whether or not ufw is enabled on boot, and in 9.04 (ufw 0.27) and later, sets the LOGLEVEL

**/etc/ufw/after.init**: initialization customization script run after ufw is initialized (ufw 0.34 and later)

**/etc/ufw/before.init**: initialization customization script run before ufw is initialized (ufw 0.34 and later)

**/var/log/ufw.log**: default location of log files

**Other Commands:**

ufw [--dry-run] [options] [rule syntax]

ufw reload **(update changes)**

ufw reset **(reset to defaults)**

**iptables**

**1. Check current settings/tables**

* sudo iptables -S
* sudo iptables -L

**2. Ensure Persistence**

* sudo apt-get install iptables-persistent