Linux Firewalls

UFW, IPTables, Firewalld

- UFW

UFW

UFW (Uncomplicated Firewall)

UFW is just a front for IPTables.

Check UFW status

```
ufw status
```

Enable UFW

```
ufw enable
```

Disable UFW

```
ufw disable
```

UFW preset rule options

UFW may have preset rulesets that can be used for applications you have installed.

View available rule presets for installed apps:

```
ufw app list
```

View available preset protocol rules

```
less /etc/services
```

You'll see an output something like:

```
Available applications:
  Apache
  Apache Full
```

```
  Apache Secure
  Nginx Full
  Nginx HTTP
  Nginx HTTPS
  OpenSSH
```

You can then use the preset options to set rules

```
UFW allow option
```

ie

```
ufw allow nginx
```

Port Rules

> When adding port/IP rules, its best practice to add a comment to ensure the rule can be clearly identified. This is done using the comment function, as an example:
> `ufw allow 80/tcp comment "web ports"`

Basic port allow rule

```
ufw allow 80/tcp
```

Basic port deny rule

```
ufw deny 80/tcp
```

Multiple port allow rule

```
ufw allow 20,21/tcp
```

Multiple port block rule

```
ufw deny 20,21/tcp
```

Port range allow rule

```
ufw allow 40000:40100/tcp
```

Port range block rule

```
ufw deny 40000:40100/tcp
```

IP Rules

```
ufw all proto TCP from IP_IP_IP_IP to any port
```

UFW Rule Ordering

UFW reads rules in order from top to bottom, with the earlier rules taking priority over subsequent rules.

View existing rules with rule numbers

```
ufw status numbered
```

Specify position in ruleset when adding rule

```
ufw insert 3 allow 80/tcp
```

The above command would add an allow rule for port 80 after rule before the existing number 3 rule.

Add rule to top of list

```
ufw prepend allow 80/tcp
```

add rule to bottom of list

```
ufw append allow 80/tcp
```

Delete a rule

```
ufw delete rulenumber
```
