Server Side 2

Firewall

- System
  - Software + Hardware
- Monitors and controls incoming and outgoing network traffic based on predefined rules.
  - How?
  - White lists?
  - Black lists?
  - iptables
    - Front end
      - ufw - Uncomplicated Firewall
- Controlling ports (services)
  - Only certain IP ranges can access a machine.
  - Only certain ports are allowed from outside a network.
  - Drop malformed packets.
  - Drop/Log multiple authentication fails.
  - Rate limiting.
  - Blocking IP addresses.

SSL (TLS)

- Create an encrypted connection between client (web browser) and web server (website).
  - mail server and mail client.
  - https://en.wikipedia.org/wiki/Transport_Layer_Security
- Establish trust.
  - Who are you?
  - Visual cues (lock + green button)
- How does it work?
  - Create a Certificate Signing Request (CSR) on your server.
    - Creates a private key and public key.
  - Send CSR file to a SSL Certificate issuer.
    - Certificate Authority (CA). Why?
  - From the CSR, CA creates a data structure to work with your private key.
    - NOTE: Private key is NEVER shared with the CA. Why?
  - CA issues the SSL certificate to install on your server.

    - An intermediate certificate is also provided to establish credibility of your SSL Certificate.
- SSL Certificates are not forever.
    - They expire.
    - They can be revoked. How?
- How does SSL Certificate Create a Secure Connection
    - https://www.digicert.com/ssl/

Self signed SSL

- What do you get?
- What do you not get?

Let's Encrypt

- https://letsencrypt.org/about/
- **Free**, **Automatic**, **Secure**, **Transparent**, Open, Cooperative.
- Automation
    - https://certbot.eff.org/
- Test SSL grade.
    - https://www.ssllabs.com/ssltest/

Demo

- SSH.
    - From Linux bash.
    - Windows Putty.
- Navigating around.
- Installing software as a Super User.
- Installing Web Server (Nginx).
- Editing files.
- View web page.
- Transfer files to VM.
- Installing certificate.