IDEO-LAB

SECURITY RULES

Guillaume oneill

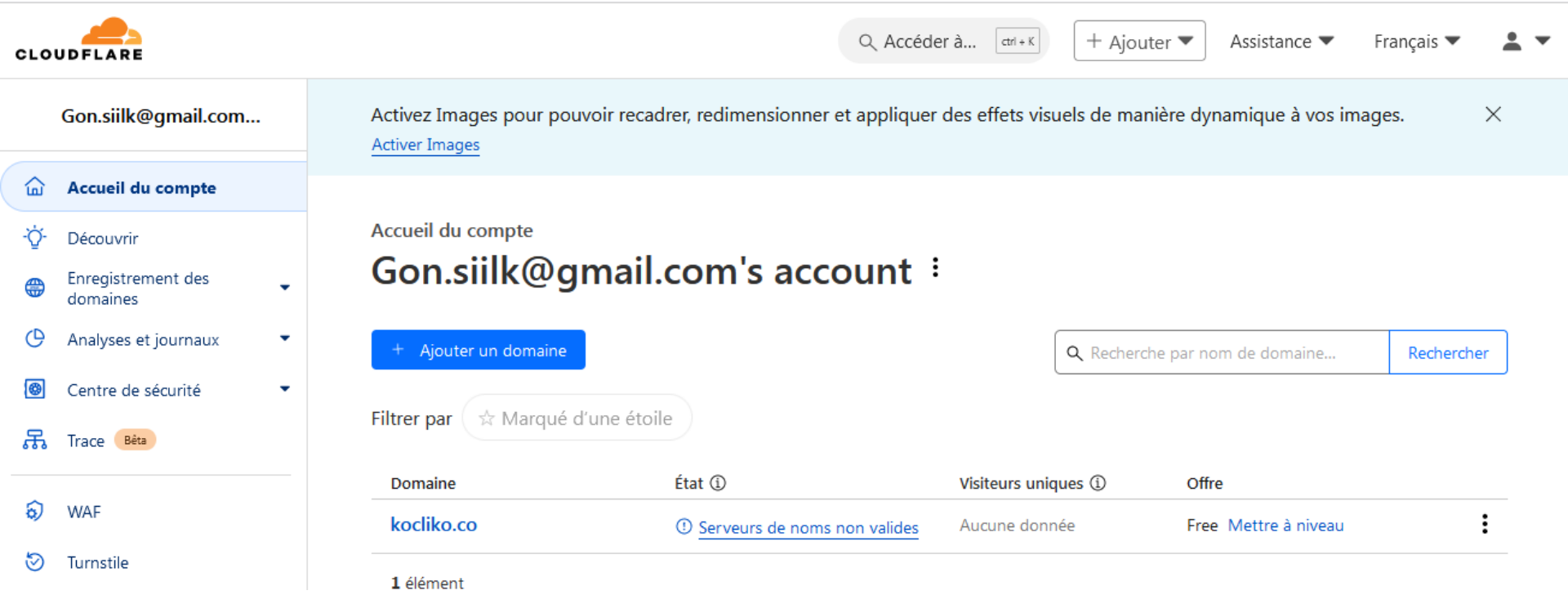
24th November 2025

Version 1.3

SECURITY

CloudFlare

- Under DNS Registrar & Reniew Payment



Firewall

Base IP Tables rules

- 1. **Limiter les connexions par IP**
- 2. **Limiter le taux de requêtes**
- 3. **Bloquer les IP malveillantes (Blacklist manuelle)**
- 4. **Protection contre le SYN Flood**
- 5. **Limiter les ping (ICMP Echo Requests)**
- 6. **Bloquer les paquets invalides**
- 7. **Protection contre les scans de port**
- 8. **Activer le mode syn-cookies**
- 9. **Journalisation des attaques**
- 10. **Sauvegarder les règles**
- **11 Drop Invalid Packets**
- **12 BLOCK COMMON ATTACK PATTERNS**

Base IPTables commands

- iptables -A INPUT -p tcp --syn --dport 80/443 -m connlimit --connlimit-above 50 -j DROP
- iptables -A INPUT -p tcp --dport 80/443 -m limit --limit 25/second --limit-burst 50 -j ACCEPTiptables -A INPUT -p tcp --dport 80/443 -j DROP
- iptables -A INPUT -s 192.168.1.100 -j DROP
- iptables -A INPUT -p tcp --syn -m limit --limit 10/second --limit-burst 20 -j ACCEPTiptables -A INPUT -p tcp --syn -j DROP
- iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/second -j ACCEPTiptables -A INPUT -p icmp --icmp-type echo-request -j DROP
- iptables -A INPUT -m state --state INVALID -j DROP
- iptables -A INPUT -p tcp --dport 0:442 -m recent --name portscan --rcheck --seconds 86400 -j DROPiptables -A INPUT -p tcp --dport 0:65535 -m recent --name portscan --set -j DROP
- net.ipv4.tcp_syncookies = 1
- iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "DDoS Attempt: " --log-level 7
- iptables-save > /etc/iptables/rules.v4
- iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP
- iptables -A INPUT -p tcp -m connlimit --connlimit-above 50 --connlimit-mask 32 -j DROP
- iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
- iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Drop Packet from Bogus IP Address

- *iptables -t mangle -A PREROUTING -s 224.0.0.0/3 -j DROP*
- *iptables -t mangle -A PREROUTING -s 169.254.0.0/16 -j DROP*
- *iptables -t mangle -A PREROUTING -s 172.16.0.0/12 -j DROP*
- *iptables -t mangle -A PREROUTING -s 192.0.2.0/24 -j DROP*
- *iptables -t mangle -A PREROUTING -s 192.168.0.0/16 -j DROP*
- *iptables -t mangle -A PREROUTING -s 10.0.0.0/8 -j DROP*
- *iptables -t mangle -A PREROUTING -s 0.0.0.0/8 -j DROP*
- *iptables -t mangle -A PREROUTING -s 240.0.0.0/5 -j DROP*

ITS JUST A SAMPLE TO BE AUTOMATED BY A PERL SCRIPT

Rules against port scanning & Rst packets

- iptables -N port-scanning
- iptables -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN
- iptables -A port-scanning -j DROP

- iptables -A INPUT -p tcp --tcp-flags RST RST -m limit --limit 2/s --limit-burst 2 -j ACCEPT iptables -A INPUT -p tcp --tcp-flags RST RST -j DROP

Block IP by countries

- sudo apt-get installl ipset
- create bash script : country_block.sh
- add list of desired country code

```
Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@ip-172-31-36-52:~# iptables-save > /etc/iptables/rules.v4
root@ip-172-31-36-52:~# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  0.0.0.0/0            0.0.0.0/0           match-set blocked_countries src
2    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 flags:0x17/0x02 #conn src/32 > 100
3    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 flags:0x17/0x02 #conn src/32 > 100
4    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:7755 flags:0x17/0x02 #conn src/32 > 100
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 limit: avg 25/sec burst 50
6    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 limit: avg 50/sec burst 100
7    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02 limit: avg 50/sec burst 100
8    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
9    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
10   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
11   ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmptype 8 limit: avg 3/sec burst 5
12   DROP       icmp --  0.0.0.0/0            0.0.0.0/0           icmptype 8
13   DROP       all  --  0.0.0.0/0            0.0.0.0/0           state INVALID
14   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpts:0:79 recent: CHECK seconds: 86400 name: portscan side: source mask: 255.255.255.255
15   LOG        all  --  0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst 5 LOG flags 0 level 7 prefix "DDoS Attempt: "
16   DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  0.0.0.0/0            0.0.0.0/0           match-set blocked_countries src
```

iptables summary –Prod server

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ip-172-31-36-52:~# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
root@ip-172-31-36-52:~# iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
root@ip-172-31-36-52:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@ip-172-31-36-52:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:http flags:FIN,SYN,RST,ACK/SYN #conn src
/32 > 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:https flags:FIN,SYN,RST,ACK/SYN #conn sr
c/32 > 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:7755 flags:FIN,SYN,RST,ACK/SYN #conn src
/32 > 100
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http limit: avg 25/sec burst 50
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https limit: avg 50/sec burst 100
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 50/sec
burst 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request limit: avg 3/sec burst 5
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       all  --  anywhere             anywhere             state INVALID
DROP       tcp  --  anywhere             anywhere             tcp dpts:0:finger recent: CHECK seconds: 86400 n
ame: portscan side: source mask: 255.255.255.255
LOG        all  --  anywhere             anywhere             limit: avg 5/min burst 5 LOG level debug prefix
"DDoS Attempt: "
DROP       tcp  --  anywhere             anywhere             #conn src/32 > 50
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PS
H,ACK,URG
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ip-172-31-36-52:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:http flags:FIN,SYN,RST,ACK/SYN #conn src/32 > 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:https flags:FIN,SYN,RST,ACK/SYN #conn src/32 > 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:7755 flags:FIN,SYN,RST,ACK/SYN #conn src/32 > 100
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http limit: avg 25/sec burst 50
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https limit: avg 50/sec burst 100
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 50/sec burst 100
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request limit: avg 3/sec burst 5
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       all  --  anywhere             anywhere             state INVALID
DROP       tcp  --  anywhere             anywhere             tcp dpts:0:finger recent: CHECK seconds: 86400 name: portscan side: source mask: 255.255.255.255
LOG        all  --  anywhere             anywhere             limit: avg 5/min burst 5 LOG level debug prefix "DDoS Attempt: "
DROP       tcp  --  anywhere             anywhere             #conn src/32 > 50
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,PSH,ACK,URG/FIN,SYN,RST,PSH,ACK,URG
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
```

Install detection tools

- Apt-get install chkrootkit
- Apt-get install tiger
- Apt-get install rkhunter (rkhunter –c –sk)
- Apt-get install packagesearch
- Apt-get install logwatch
- Apt-get install tcptrack
- https://www.cyberciti.biz/faq/block-entier-country-using-iptables/
- *ifconfig*
- *tcptrack –i ens5*

Ddos attach prevention

iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP

iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j DROP

iptables -t mangle -A PREROUTING -p tcp -m conntrack --ctstate NEW -m tcpmss ! --mss 536:65535 -j DROP

iptables -t mangle -A PREROUTING -p icmp -j DROP

https://javapipe.com/blog/iptables-ddos-protection/

https://javapipe.com/blog/iptables-ddos-protection/

iptables -A INPUT -p tcp -m connlimit --connlimit-above 80 -j REJECT --reject-with tcp-reset

iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j ACCEPT

iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j DROP

iptables -t mangle -A PREROUTING -f -j DROP

Doos attack iptables last rules

- ### 5: Block spoofed packets ###
- /sbin/iptables -t mangle -A PREROUTING -s 224.0.0.0/3 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 169.254.0.0/16 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 172.16.0.0/12 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 192.0.2.0/24 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 192.168.0.0/16 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 10.0.0.0/8 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 0.0.0.0/8 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 240.0.0.0/5 -j DROP
- /sbin/iptables -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j DROP
-
- ### 6: Drop ICMP (you usually don't need this protocol) ###
- /sbin/iptables -t mangle -A PREROUTING -p icmp -j DROP
-
- ### 7: Drop fragments in all chains ###
- /sbin/iptables -t mangle -A PREROUTING -f -j DROP
-
- ### 8: Limit connections per source IP ###
- /sbin/iptables -A INPUT -p tcp -m connlimit --connlimit-above 111 -j REJECT --reject-with tcp-reset
-
- ### 9: Limit RST packets ###
- /sbin/iptables -A INPUT -p tcp --tcp-flags RST RST -m limit --limit 2/s --limit-burst 2 -j ACCEPT
- /sbin/iptables -A INPUT -p tcp --tcp-flags RST RST -j DROP
-
- ### 10: Limit new TCP connections per second per source IP ###
- /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j ACCEPT
- /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j DROP
-

Install a Firewall

- Apt-get install iptables
- Apt-get install portsentry
- Apt-get install nmap
- Apt-get install fail2ban

- Limit Flood or Service deny
- Limit scan ports
- Limit connections per sec/IP
- Denny Ip address
- Server Intrusion (portsentry/Iptables)
  - Portsentry –audp
  - Portsentry -atcp
- Scan Currently Opened Ports (nmap)
  - Both servers PX90 and PX120
- Set in crontab an antivirus scanner
  - Virus « IptabLex » and « IptabLes »

```
#!/bin/sh

# Réinitialise les règles
sudo iptables -t filter -F
sudo iptables -t filter -X

# Bloque tout le trafic
sudo iptables -t filter -P INPUT DROP
sudo iptables -t filter -P FORWARD DROP
sudo iptables -t filter -P OUTPUT DROP

# Autorise les connexions déjà établies et localhost
sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -t filter -A INPUT -i lo -j ACCEPT
sudo iptables -t filter -A OUTPUT -o lo -j ACCEPT

# ICMP (Ping)
sudo iptables -t filter -A INPUT -p icmp -j ACCEPT
sudo iptables -t filter -A OUTPUT -p icmp -j ACCEPT

# SSH
sudo iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT

# DNS
sudo iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

# HTTP
sudo iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

# FTP
sudo iptables -t filter -A OUTPUT -p tcp --dport 20:21 -j ACCEPT
sudo iptables -t filter -A INPUT -p tcp --dport 20:21 -j ACCEPT

# Mail SMTP
iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 25 -j ACCEPT

# Mail POP3
iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 110 -j ACCEPT

# Mail IMAP
iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT

# NTP (horloge du serveur)
sudo iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT
```

How to Check overloading server

- *#!/bin/bash*
- ip="148.251.238.138"
- port="80"
- **for** i **in {**1..100**}**
- **do** # ***do*** *nothing just connect and exit*
  echo "exit" | nc ${ip} ${port};
- **done**

New Iptables rules by country

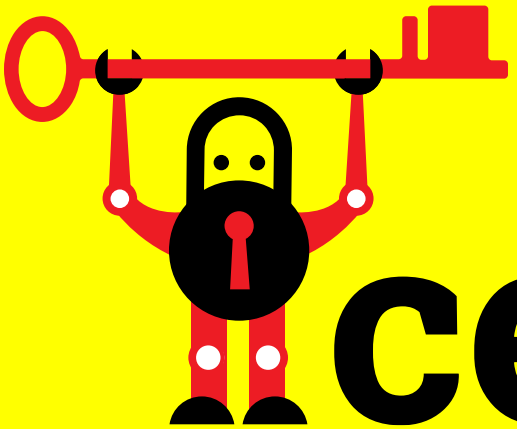
```
# ----------------------------------------
# ---- Block all Chineses IP address   ---
# ----------------------------------------
counter=1
ISO="cn ru kr"
IPT=/sbin/iptables
WGET=/usr/bin/wget
EGREP=/bin/egrep
SPAMLIST="countrydrop"
ZONEROOT="/root/iptables"
DLROOT="http://www.ipdeny.com/ipblocks/data/countries"
$IPT -F $SPAMLIST
[ ! -d $ZONEROOT ] && /bin/mkdir -p $ZONEROOT
$IPT -N $SPAMLIST
for c  in $ISO
do
        tDB=$ZONEROOT/$c.zone
        #$WGET -O $tDB $DLROOT/$c.zone
        SPAMDROPMSG="$c Country Drop"
        BADIPS=$(egrep -v "^#|^$" $tDB)
        for ipblock in $BADIPS
        do
          $IPT -A $SPAMLIST -s $ipblock -j DROP
          counter=`expr $counter + 1`
        done
done
$IPT -I INPUT -j $SPAMLIST
$IPT -I OUTPUT -j $SPAMLIST
$IPT -I FORWARD -j $SPAMLIST
iptables -L -n
echo "ADDED " $counter " IP Address Blocks"
```

TO DO LIST

- AUTOMATE LOGWATCH ANALYZE
- KERNEL PARAMETERS TUNING
- REGULAR MONITORING (TOOLS)
- CLOUDFLARE DNS REGISTRAR

SSL HTTPS

ssl Https



certbot

Certbot and Let's encrypt

- sudo apt-get update
- sudo apt-get install software-properties-common
- sudo add-apt-repository ppa:certbot/certbot
- sudo apt-get update
- sudo apt-get install certbot

- ********** IF ERROR ****
- **python3 -m pip install cffi**
- **python3 -m pip install certbot-nginx**

- If already installed, good to desinstall and reinstall again

sudo certbot –nginx

sudo certbot --nginx certonly –d staging.ideo-lab.com -d staging.ideo-lab.co

NGINX Settings

```
# --------------------------------
# --------------------------------
# --- SSL Settings             ---
# --------------------------------
# --------------------------------
ssl_enable = False
SECURE_SSL_REDIRECT = False
SESSION_COOKIE_SECURE = False
CSRF_COOKIE_SECURE = False

SSL_URLS = (
    '^/login/',
        # ...
    )

SSL_IGNORE_URLS = (
    '^/i18n_js$',
    '^/static/',
        # ...
    )

if ssl_enable:
    SECURE_SSL_REDIRECT = True
    SESSION_COOKIE_SECURE = True
    CSRF_COOKIE_SECURE = True
    SECURE_HSTS_SECONDS = 31536000
    SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')
    SECURE_REDIRECT_EXEMPT = [
    ]
```

NGINX Settings

```
# ------------------------------------------------
   # ---  S S L   Settings for nginx                ---
   # ------------------------------------------------
   ssl on;
   ssl_certificate  /etc/letsencrypt/live/www.ideo-lab.com/fullchain.pem;
   ssl_certificate_key /etc/letsencrypt/live/www.ideo-lab.com/privkey.pem;
   ssl_trusted_certificate  /etc/letsencrypt/live/www.ideo-lab.com/chain.pem;
   include /etc/letsencrypt/options-ssl-nginx.conf;
   ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

   ssl_stapling on;  .
   ssl_stapling_verify on;
   ssl_protocols    SSLv3  TLSv1  TLSV1.1  TLSv1.2;
   ssl_ciphers EECDH+AESGCM:EECDH+CHACHA20:EECDH+AES;
   ssl_session_cache builtin:1000  shared:SSL:10m;
   ssl_ecdh_curve secp384r1;
   ssl_prefer_server_ciphers on;

   ## TLS parameters
   ssl_session_cache shared:SSL:10m;
   ssl_session_timeout 5m;
   ssl_session_tickets off;
```