



Security Technology Chessboard

RESCUE PEOPLE AS SAINT

Huynh Quoc Viet Quang

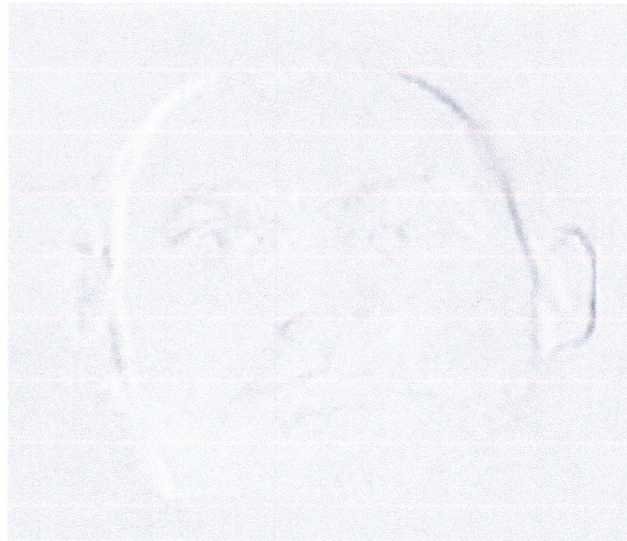
USPTO Trademarks (<https://uspto.report/TM/>) ›

/ Huynh Quoc Viet Quang (<https://uspto.report/company/Huynh+Quoc+Viet+Quang>) ›

/ Rescue People As Saint Application #88765425 (<https://uspto.report/TM/88765425/>)

Application Filed: 2020-01-19 (2020-01-19)

Trademark Application Details



The mark consists of RESCUE THE SOCIETY, RESCUING HUMANS, ENVIRONMENTAL RESCUE, TECHNOLOGICAL RESCUE.

Mark For: RESCUE PEOPLE AS SAINT™ trademark registration is intended to cover the category of psychological research.

Status



LIVE APPLICATION Awaiting Examination

2020-01-22 UTC

☐ Refresh

([/TM/88765425/refresh](https://uspto.report/TM/88765425/refresh))

The trademark application has been accepted by the Office (has met the minimum filing requirements) and has not yet been assigned to an examiner.


Serial Number	88765425
Mark Literal Elements	RESCUE PEOPLE AS SAINT
Mark Drawing Type	-
Mark Type	Service Mark
Standard Character Claim	No
Current Location	NEW APPLICATION PROCESSING 2020-01-22
Basis	1(a)
Class Status	ACTIVE
Primary US Classes	<div>100: Miscellaneous</div> <div>101: Advertising and Business</div>
Primary International Class	<div>042 - Primary Class</div> <div>(Computer, scientific & legal) Scientific and technological services and research and design relating thereto: industrial analysis and research services; design and development of computer hardware and software; legal services.</div>
Filed Use	Yes
Current Use	Yes
Intent To Use	No
Filed ITU	No

44D Filed	No
44E Current	No
66A Current	No
Current Basis	No
No Basis	No

Timeline

2020-01-18	Date of First Use
2020-01-18	Date of Use In Commerce
2020-01-19	Application Filed
2020-01-22	Location: NEW APPLICATION PROCESSING
2020-01-22	Status: Live/Pending
2020-01-22	Status: New application will be assigned to an examining attorney approximately 3 months after filing date.
2020-01-22	Transaction Date

Trademark Ownership

Owner:	 Huynh Quoc Viet Quang (/company/Huynh+Quoc+Viet+Quang)
Address	315 133rd Street S Tacoma, WASHINGTON UNITED STATES 98444
Legal Entity Type	Individual

Documents

 Drawing (/TM/88765425/DRW20200122072403/)	IMAGE/JPEG	2020-01-19
 Specimen (/TM/88765425/SPE20200122072403/)	IMAGE/JPEG	2020-01-19
 TEAS Plus New Application (/TM/88765425/FTK20200122072403/)	APPLICATION/XML,IMAGE/JPEG	2020-01-19

Design Search Codes

020101	Heads of men facing forward; Portraiture of men facing forward; Men
020102	Silhouettes of men; Men depicted as shadows or silhouettes of men
260921	Squares that are completely or partially shaded

Attorney of Record

HUYNH QUOC VIET QUANG
 315 133RD STREET S
 TACOMA, WA 98444

Good, Services, and Codes

International Codes:	42
U.S. Codes:	100,101

Type Code	Type
DM0000	The mark consists of RESCUE THE SOCIETY, RESCUING HUMANS, ENVIRONMENTAL RESCUE, TECHNOLOGICAL RESCUE.

Trademark Filing History

Description	Date	Proceeding Number
NEW APPLICATION ENTERED IN TRAM	2020-01-22	

SECURITY TECHNOLOGY CHESSBOARD

TinyLinux Firewall

System myRules

Custom Rules

Install Text Editor

`yum install nano`

Open Up Custom Rules

`nano /etc/tinylinuxfirewall/rules.sh`

Add Custom Rules

`iptables -A INPUT -p tcp -s YOUR.SERVERIP.HERE --dport 22 -j ACCEPT`

`iptables -A INPUT -p tcp -s YOUR.HOMEIP.HERE --dport 22 -j ACCEPT`

`iptables -A INPUT -p tcp --dport 22 -j DROP`

Save file: `Ctrl + o`

Enter

`Ctrl + x`

Call Service

service tlfd

or

sh /etc/tinylinuxfirewall/Firewall/firewall.sh

Choose 1, 2, 3 (option)

Enter

Compress Linux

Application Level: Use tinylinux firewall

Open tinylinux firewall custom rules

nano /etc/tinylinuxfirewall/rules.sh

Add custom rules:

iptables -A INPUT -p tcp -s YOUR.SERVERIP.HERE --dport 22 -j ACCEPT

iptables -A INPUT -p tcp -s YOUR.SERVERIP.HERE --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -j DROP

Save file: Ctrl + o

Enter

Ctrl + x

Restart tinylinux firewall service

service tlfed

Choose 1, 2, 3 (option)

Enter

Server Level: Use tcp-wrappers (hosts.allow and hosts.deny)

Enable remote access you must whitelist your two servers

To allow ip

nano /etc/hosts.allow

Add:

sshd :

sshd : YOUR.SERVERIP.HERE : allow

sshd : YOUR.SERVERIP.HERE : allow

: allow

Save file: Ctrl + o

Enter

Ctrl + x

To deny all

nano /etc/hosts.deny

Add:

sshd: ALL

Save file: Ctrl + o

Enter

Ctrl + x

Restart ssh service

service sshd restart

Network Level: Use remote access

Connect two remote servers via password you must have two servers

ssh root@serverip -p 22

Enter

Enter your server password

Iptables Routing As Reverse Proxy

Installation

Choose firewall, copy and paste to server

Open Up Custom Rules

nano /etc/tinylinuxfirewall/rules.sh

Add Custom Rules

iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

```
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A TLF-SYN-FLOOD -p tcp -m tcp --dport 80 -j ACCEPT
```

```
iptables -I TLF-SYN-FLOOD -p tcp -m tcp --dport 80 -j ACCEPT
```

```
iptables -A TLF-SYN-FLOOD -p tcp -m tcp --dport 81 -j ACCEPT
```

```
iptables -I TLF-SYN-FLOOD -p tcp -m tcp --dport 81 -j ACCEPT
```

```
##RemoteServer## iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination  
$ip:80
```

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 81
```

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Save file : Ctrl + o

Enter

Ctrl + x

Restart tinylinux firewall

service tlfld

Choose 1, 2, 3 (option)

Enter

Nginx Reverse Proxy

Step 1.

Install Tinylinux Firewall Version 3.2 Compile

Copy And Paste the link

Step 2.

Install Tinylinux Firewall Version 2.1 Webpanel

Copy And Paste the links

Stop httpd service

service httpd stop

Step 3.

Compile, login with ssh go to tinylinuxfirewall management

cd /etc/tinylinuxfirewall/

ls

cd Compile

sh install.sh

Step 4.

Change port of web Server, Nginx always in front of Httpd Web Server if you run reverse proxy

Nginx keeps port 80

Httpd port (anything)

Nginx

Port 80 in file /etc/nginx/nginx.conf

Listen 80

Step 5.

Change httpd port /etc/httpd/httpd.conf

nano /etc/httpd/conf/httpd.conf

Look for "Listen 80" change to 81

Save file: Ctrl + o

Enter

Ctrl + x

Step 6.

NGINX New Compile - Web Server Needs Security

```
cd /etc/tinylinuxfirewall/
```

```
ls
```

```
cd WebserverFirewall
```

Secure NGINX choose option: 2

```
sh Cinstall.sh
```

Restart two web servers

```
service nginx restart & service httpd restart
```

Test Links:

<http://155.138.220.42:80> /upload content index.html to HTTPD
/usr/share/nginx/yourdomain/public_html

NGINX only use for send traffics to HTTPD so no need to host storage.

<http://155.138.220.42:81> /upload content index.html to HTTPD
/var/www/yourdomain/public_html

Step 7.

Create HTTPD your hosting account

```
cd /etc/tinylinuxfirewall/
```

```
cd AccountPanel
```

```
sh createaccount.sh
```

Example:

```
cd /root
```

```
chmod 0755 httpd.sh
```


`sh httpd.sh domain.com`

Create just 1 hosting account (only HTTPD)

Step 8.

Open `domain.com.conf` in `/etc/httpd/conf.d/` to change port

`cd /etc/httpd/conf.d`

`ls`

`nano yourdomain.com.conf`

Look for "Listen 80" change to 81

Save file: `Ctrl + o`

`Enter`

`Ctrl + x`

Step 9.

Require, create a reverse proxy domain in `nginx` to pass traffics to `httpd`

```
cd /etc/tinylinuxfirewall/
```

```
cd ReverseProxyPanel
```

```
ls
```

```
sh reverseproxyserver.sh
```

Example:

```
cd /root
```

```
chmod 0755 ip_reverse.sh
```

```
sh ip_reverse.sh 155.138.220.42
```

```
cd /root
```

```
chmod 0755 nginx_reverse.sh
```

```
sh nginx_reverse.sh domain.com
```

Step 10.

Change port of the domain.com.conf to httpd port 81

```
cd /etc/nginx/conf.d
```

```
ls
```

```
nano yourdomain.com.conf
```

Look for proxy_pass <http://ip:80> change to proxy_pass <http://ip:81>. This is load balance you must edit 3 proxy_pass.

Step 11.

Control Traffics With TinyLinux Firewall

Open Up Custom Rules

```
nano /etc/tinylinuxfirewall/rules.sh
```

Add Custom Rules

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A TLF-SYN-FLOOD -p tcp -m tcp --dport 80 -j ACCEPT
```

```
iptables -I TLF-SYN-FLOOD -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A TLF-SYN-FLOOD -p tcp -m tcp --dport 81 -j ACCEPT
iptables -I TLF-SYN-FLOOD -p tcp -m tcp --dport 81 -j ACCEPT
##RemoteServer## iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
                    $ip:80
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 81
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Step 12.

Before Test

Upload index.html page and ready for testing

Step 13.

Restart Tinylinux Firewall

service tlfd

Choose 1,2,3 option

Enter

Exit: Ctrl + c

Step 14.

Restart two webservers

`service nginx restart & service httpd restart`

Finished

If it shows error page 403 that mean no content index.html file

Any issue checking:

1. Change httpd and nginx port

`/etc/httpd/conf/httpd.conf` Listen 81

`/etc/httpd/conf.d/domain.com.conf` <VirtualHost *:81>

`/etc/nginx/conf.d/domain.com.conf` proxy_pass <http://155.138.220.42:81>;

Load balance you must edit 3 proxy_pass

2. Nginx issue checking:

May forget to install webserver firewall for nginx

3. Upload the index.html page the default no content in storage.


Notary

Name: Huynh Quoc Viet Quang

Signature: 

Date: Feb 8, 2021



State of WA County of Pierce
The foregoing instrument was acknowledged before me
on this 8th day of February, 2021
by Huynh Quoc Viet Quang

Notary Public Signature

