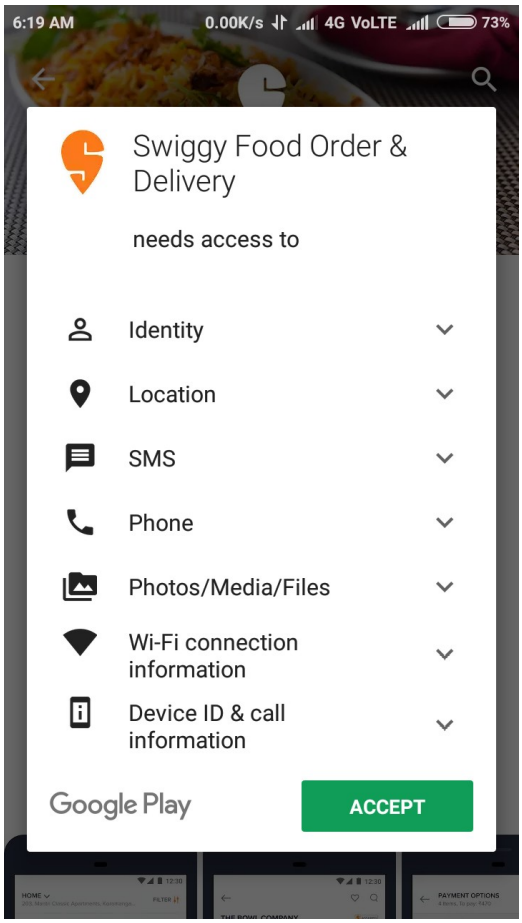
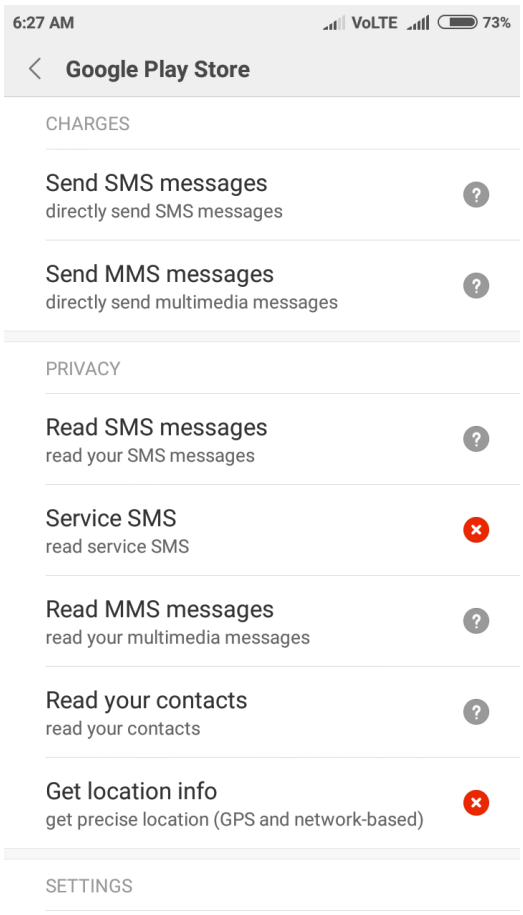
# Mobile Privacy

Mobile Apps we all love and use on daily basis . And on average we have 26 Apps installed by us and near about 20 apps are pre-installed . In the Android operating system, “permissions” are what app developers use to inform users about how the app will interact with the device and personal information . We accepts those permissions when we install those apps .




Note :- We never have choice to accept permissions for pre-installed apps . And most of those apps belongs to google .

Game of permissions :-

- 29 applications were found to request the exact same permissions as applications that are known to be spyware .
- A full eight applications explicitly request a specific permission that would allow the device to brick itself, or render it absolutely unusable .
- **383 applications were found to have the ability to read or use the authentication credentials from another service or application .**
- Finally, 3% of all of the Market submissions that have been analyzed could allow an application to send unknown premium SMS messages without the user's interaction or authorization.

Sources :- http://gizmodo.com/5570942/one-in-five-android-apps-access-your-private-data

Outcomes of Permission game :-

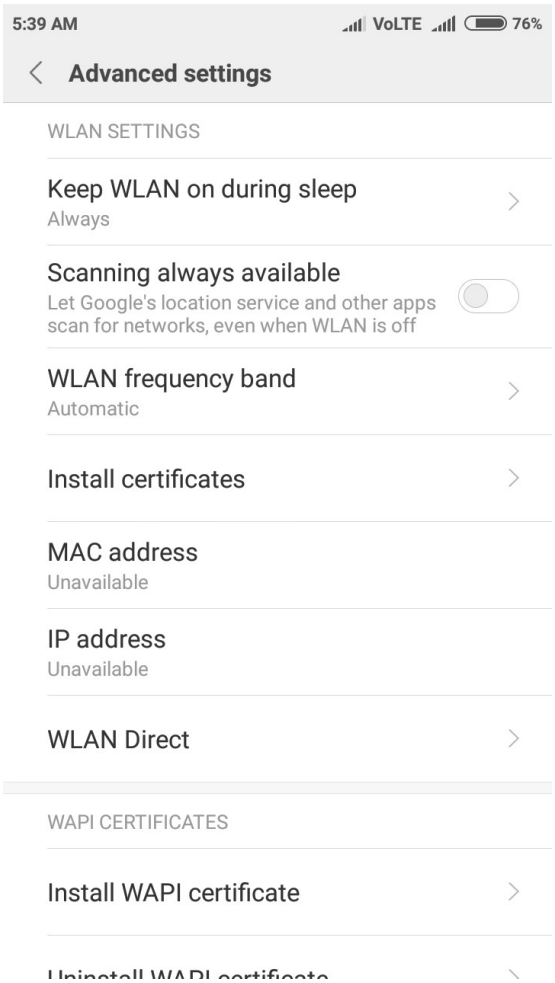
- Simply by requesting access to the permissions "Internet" and "Access_Wifi_State," an application could identify the phone through the MAC address of its Wi-Fi adapter and track its movements around the world.

Sources :- http://www.infoworld.com/article/2859565/mobile-technology/android-apps-exploit-permissions-to-access-personal-info-researchers-find.html

Question . Do all these permissions are necessary for the app to work properly ?
Answer No .

Question . Can we remove unnecessary permissions for any app ?
Answer . Yes , We can control their permissions and choose what should be permitted and what shouldn't be . ( It depends on mobile vendor )

If you check what permissions we have allowed till now you will be shocked , for example




Why would google want to scan for networks around us even though google have permission to access GPS data ?
For example if you turned GPS off , with wifi network data it can still figure out where are you .

I am not a terrorist so why should I be worried about all these permissions ?
You are just a product for the companies outside and all of your private information is being sold out ?
I can't say anything about surveillance now ?

More about permissions :-

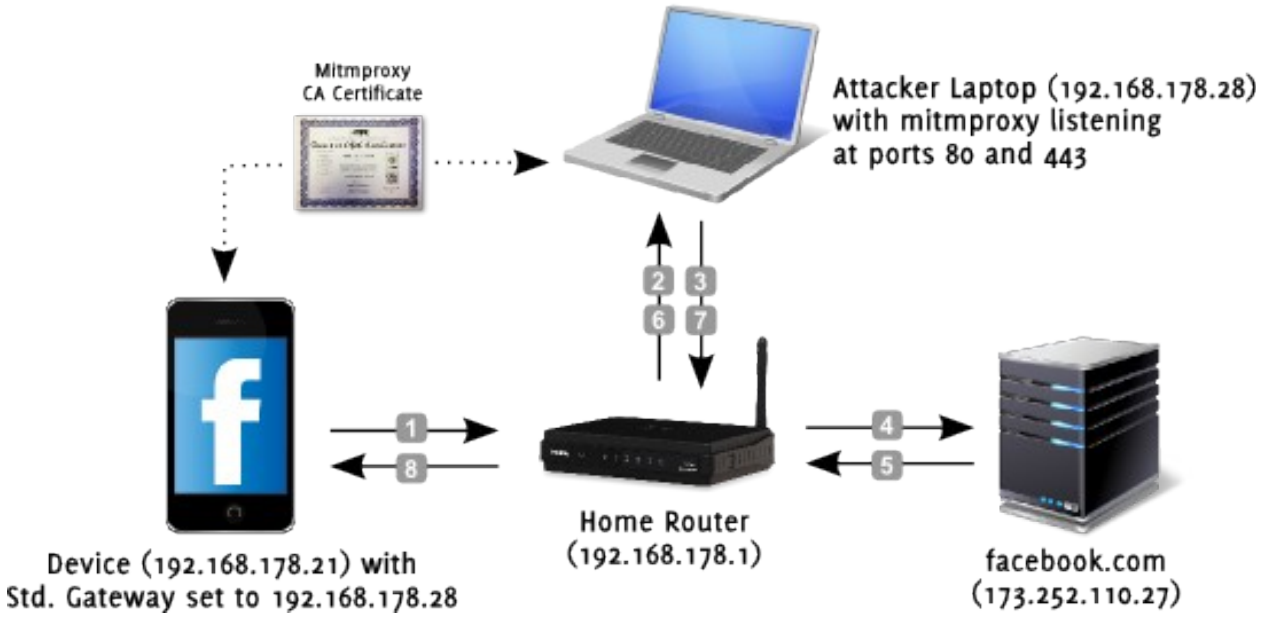
**The most common Android app permissions allow access to a smartphone's internet connectivity .** The average app requested five permissions before installation, and the two most common permissions sought by Android apps help those apps access the internet. These include the "Full network access" permission (used by 83% of apps), which allows an app to access whatever network the device is connected to at the time, as well as the "View network connections" permission (used by 69% of apps). The latter type of permission enables an app to see what networks the device is able to access. The third- and fourth-most-common permissions allow apps to access memory or available storage on the phone, a feature apps would need in order to save content to the device.


**Most Android app permissions seek access to a device's hardware, rather than a user's personal information .** Of the 235 distinct types of permissions associated with apps in the Google Play Store, most (165) relate to allowing an app access to the device's hardware, such as allowing the app to control the camera flash or prevent the device from going to sleep, while 70 app permissions could allow access to personal information. Personal information in this context relates to getting a user's precise location using GPS or reading data about your contacts stored on your device.

Source :- http://www.pewresearch.org/fact-tank/2015/11/10/key-takeaways-mobile-apps/

My Experiment :-

I intercepted traffic going out a android device using proxy server . For that purpose I generated a root CA certificate and installed it on the target device . Certificate can generated using openssl program from linux . Although I used BurpSuite for intercepting proxy . Squid program linux can also be used for that purpose . Also I used ssl_bump so that I can interfere with HTTPS traffic .




What we did :-

- Captured 673 HTTP and HTTPS requests from single android
- 3 hours experiment
- some apps were accessed voluntarily

Observation :-

- 411 requests were HTTPS and 262 were HTTP only
  → this signifies that approx 33% of your data is not safe
- 73 no. of unique domains visited
  → 22 domains out of 73 belongs to google i.e. approx 30%
- 113 requests were static requests i.e. .js , .txt etc no useful data
  → must have been generated by using browser
- 44 requests used google advertising id for their business
- Advertisers uses following Ids to identify the device in particular :-
  1. Google Advertising Id
  2. Mac Address
  3. device Token
  4. device Finger Print Id etc

  → so once you install any of these apps you can't perform any crime from that device . Or Its easy for police to catch criminals if device has ever been used . Its android forensics .

# Detailed Analysis of Domains Accesses :-

## List of domains accessed by Android including services and advertisements :-

- **clients3.google.com** google
  some gms app was acessing it with your gmail account
- **m.orkut.com** google
  don't why it is still here
- **dev.appboy.com** its tool allows app developers to segment and analyze their users for the purposes of improving marketing effectiveness and creating customized experiences.
  foodpanda was using it.
- **ip-api.com** geolocation api
  some access it **??**
- **www.estrongs.com** Es file explorer
  it was sending some data in form of numbers **???**
- **apiv2.moengage.com** MoEngage - User analytics & Engagement .
  swiggy was using it and it was accessing your location
- **api.accuweather.com** Instant, Free Access to AccuWeather APIs for Developers .
  may be your was accessing it.
- **ogs.google.com** google
  asus browser was posting some data based on user mobile id's
- **blog.whatsapp.com** whatsapp
  voluntarily access by web
- **scontent.xx.fbcdn.net** facebook
  facebook content deleviry network
- **189358.engine.mobileapptracking.com** Mobile Analytics and Performance Marketing Platform I TUNE
  phonepe was using it **???**
- **fonts.gstatic.com** google

- **trends.google.com** google
- **accounts.google.com** google
- **enquiry.indianrail.gov.in** indian railways
  it uses http i.e. session id in plain text
- **versioncheck-bg.addons.mozilla.org**
- **www.googleapis.com**
- **pubads.g.doubleclick.net** google ads
  youtube was using it
- **mail.google.com**
- **b-www.facebook.com**
- **phonepe.helpshift.com** phonepe
- **reports.crashlytics.com** app analytics
  swiggy is using it for crash analytics . tracelogs are sent to reports.crashlytics.com .
- **clients1.google.com** google
  used by google chrome don't know why **?**
- **detectportal.firefox.com** firefox
  for checking internet connectivity
- **m.youtube.com** youtube
- **stats.appsflyer.com** Data-driven marketers rely on AppsFlyer for independent measurement solutions and innovative tools to grow their mobile business
  swiggy was using it
- **www.youtube.com** youtube
- **self-repair.mozilla.org**
- **accounts.youtube.com**
- **events.appsflyer.com** Data-driven marketers rely on AppsFlyer for independent measurement solutions and innovative tools to grow their mobile business
  was accessing device network info
- **static.xx.fbcdn.net** facebook

- **portal.fb.com** facebook
- **api.swiggy.in**
- **graph.facebook.com**
- **www.gstatic.com**
- **firefox.settings.services.mozilla.com**
- **ssl.gstatic.com**
- **app.adjust.com** Adjust is the business intelligence platform mobile app marketers love : we combine attribution for advertising sources with advanced in-app analytics and store statistics for unbeatable marketing insights .
  it was posting device location and basic information to
- **spns.swiggy.com** swiggy
  it posts your IEMI no. , mac address and much more to swiggy database and don't know why ? Is it legal ?
- **in-public.foodapi.io** foodpanda
  may be basic api for foodpanda
- **b-graph.facebook.com** facebook
  used for authentication of user for facebook app or messenager app
- **faq.whatsapp.com**
- **rts.mobula.sdk.duapps.com** DU Group - The World Most Trusted Android App Develope
  used by es explorer for some wifi stuff
- **api.parse.com** aquired indirectly by facebook
  posting user device information like IMEI , serial number , GCMSenderId etc highly confidential data for any user .
- **app.hotline.io** Hotline now powers in-app chat across Android, iOS, Phonegap, Unity and also supports Facebook Messenger
  used by swiggy for some chat management
- **gmail.com** google mail accounts
- **e.crashlytics.com** app analytics
  posting application/vnd.crashlytics.android.events file to their server for analysis

- **services.addons.mozilla.org**
- **www-cdn.whatsapp.net**
- **aus5.mozilla.org**
- **api.push.go2reach.com**
- **googleads.g.doubleclick.net**
- **pasta.esfile.duapps.com**
- **www.telize.com**
- **m.facebook.com**
- **www.google.com**
- **blocklist.addons.mozilla.org**
- **www.whatsapp.com**
- **api.swiggy.com**
- **t.appsflyer.com**
- **hmma.baidu.com**
- **analytics.query.yahoo.com**
- **android.clients.google.com**
- **api.foodpanda.com**
- **edge-chat.facebook.com**
- **de-docs.s3.amazonaws.com**
- **www.google-analytics.com**
- **play.googleapis.com**
- **conf.international.baidu.com**
- **settings.crashlytics.com** The most powerful, yet lightest weight crash reporting solution

for iOS and Android developers. | Crashlytics

- **rt.api.glispa.com** Glispa Global Group - The Global, Mobile Ad Tech Company that Guarantees Results
- **mobile-collector.newrelic.com** Mobile App Performance Monitoring for iOS and Android | New Relic Mobile

# How user data looks on the wire :-

## spns.swiggy.com :-

POST /analytics/transactional/device/add HTTP/1.1\r\nAccept: application/json; charset=utf-8\r\napp-version: 1.7.11\r\nversion-code: 156\r\ntoken: bkjbdkjasb\r\nTid: csnbb-ascsd- s-dvsd-vsd-dv\r\nos-version: 5.0\r\ndeviceId: 533513132132132\r\nswuid: f59df4d0c9247998\r\nUser-Agent: Swiggy-Android\r\nConnection: close\r\nContent-Type: application/json; charset=UTF-8\r\nContent-Length: 576\r\nHost: spns.swiggy.com\r\nX-NewRelic-ID: dashkfjbkjfbckjsdbvkj\r\n\r\n{"customerId":"4719033","device":{"appId":"in.swiggy.android","carrier":"Reliance","device":"357996060367586","deviceTz":"India Standard Time","deviceTzOffset":"+0530","deviceToken":"bifdjcbkjbckjbskjcbkjbcjadsacscdvsdvsdvsdv","imei":"357996060367586","macAddress":"f0:79:59:ac:8c:84","manufacturer":"asus","model":"ASUS_T00J","os":"android","osVersion":"5.0","product":"WW_a501cg","densityDpi":2.0,"deviceTs":1.4983783E12,"height":1280,"osApiLevel":21,"width":720}}c

note :- if police finds a device broken or formatted they can use this information which is stored in spns.swiggy.com servers or similar servers .

## events.appsflyer.com :-

"device":"ASUS_T00J1","firstLaunchDate":"2017-06-22_1444+0530","installDate":"2017-06-22_1444+0530","sdk":"21","referrer":"utm_source=direct&utm_medium=direct&utm_campaign=direct","carrier":"Reliance","deviceFingerPrintId":"ffffffff-86f3-09f2-ffff-ffffa09bb158","date1":"2017-06-

22_1444+0530","af_preinstalled":"false","advertiserIdEnabled":"true","iaecounter":"9","lang_code":"en",,"af_events_api":"1","platformextension":"android_native","network":"WIFI","operator":"AIRCEL","country":"US","date2":"2017-06-22_1444+0530","brand":"asus","prev_event":"{\\"prev_event_timestamp\\":\\"1498377214199\\",\\"prev_event_value\\":\\"{\\\\\\"sid\\\\\\":\\\\\\"8366f16d-54db-45c4-9cdc-86e16ffcccb1\\\\\\",\\\\\\"customer_user_id\\\\\\":\\\\\\"scsxvdsvdsvfsd \\\\\\",\\\\\\"tid\\\\\\":\\\\\\"vbnvadnvasdjhsbdjh-scnsmnsc'\\\\\\"}\\",\\"prev_event_name\\":\\"af_app_launch\\"}","af_timestamp":"1498377309746","uid":"bjh151121-4452scsdvc","isFirstCall":"false","counter":"37","model":"ASUS_T00J","product":"WW_a501cg"

## app.adjust.com :-

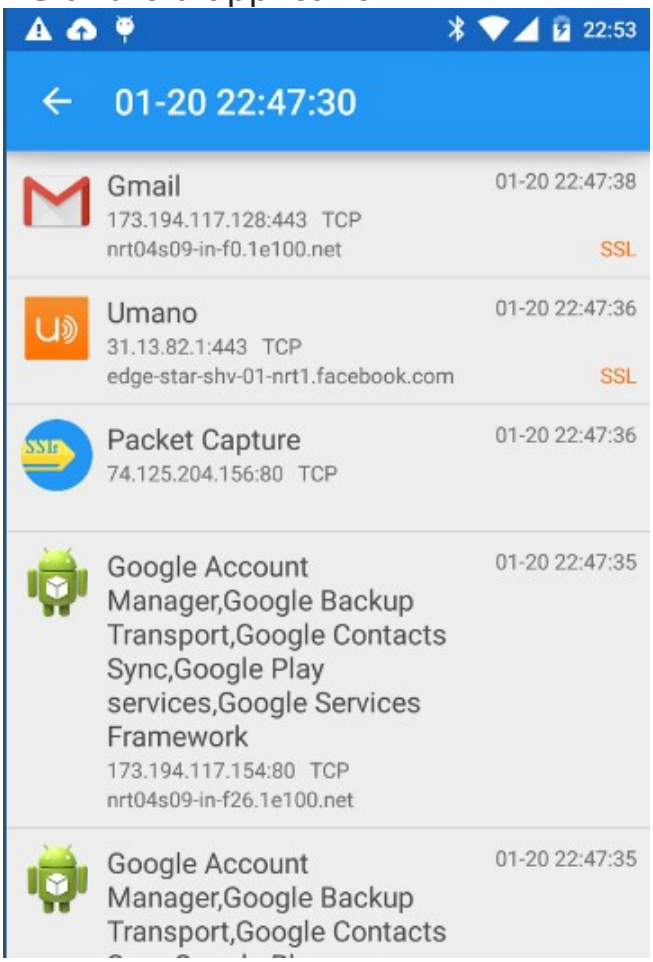
POST /session HTTP/1.1\r\nClient-SDK: android4.11.2\r\nUser-Agent: Dalvik/2.1.0 (Linux; U; Android 5.0; ASUS_T00J Build/LRX21V)\r\nHost: app.adjust.com\r\nConnection: close\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: 1556\r\n\r\nupdated_at=2017-06-22T15%3A18%3A53.371Z&country%22%3A%22India%22%2C%22device_manufacturer%22%3A%22asus%22%2C%22area_id%22%3A%22431699%22%2C%22city%22%3A%22Gurgaon%22%2C%22area_name%22%3A%22Patel+Nagar+%28Patel+Nagar%29%22%7D&installed_at=2017-06-22T15%3A18%3A53.371Z%2B0530&app_version=1.0.7&country=US&screen_size=normal&app_token=qmu1bzh6wi68&device_name=ASUS_T00J&created_at=2017-06-25T13%3A43%3A20.636Z%2B0530&display_height=1280&language=en&os_version=5.0&last_interval=158197&cpu_type=x86&sent_at=2017-06-25T13%3A43%3A22.243Z%2B0530

## api.parse.com :-

POST /1/installations HTTP/1.1\r\nContent-Type: application/json\r\nX-Parse-Application-Id: KjTIjvbXB2Hmq2xsKOJqnoMvb0NeL9R4C5BKspPP\r\nX-Parse-Client-Key: FFTUIpxtfKZ4JLtAwZ8j4QXkMGS8s7ibdyUaoLva\r\nUser-Agent: Dalvik/2.1.0 (Linux; U; Android 5.0; ASUS_T00J Build/LRX21V)\r\nHost: api.parse.com\r\nConnection: close\r\nContent-Length:

817\r\n\r\n{"deviceToken":"dN4hT5EikRg:APA91bHwFcqYdjzpfJ26Ou4jTlKpYAbcikCIr294HlIvBpiHHC6CV3qSHLAYVbLHz_s2KlVq7VpHR-Q_Dbhjvjvhvshdvw23432bnvhvNsyUeGpGfJETjiV-SIgn","installationId":"f5dfs7-3440-4784-8b8c-833f76cb68a9","deviceType":"android","pushType":"gcm","GCMSenderId":"745199028400","lang":"en_US","country":"IN","model":"ASUS_T00J","rom_version":"LRX21V.ASUS_T00J_WW_user_3.24.40.87_20151222_34 release-keys","screenSize":"720x1280","screenWidth":720,"screenHeight":1280,"screenInches":5,"serialNumber":"ECAZFG451176","sdkVersionCode":1240,"sdkVersionName":"1.2.4","appVersionCode":1520101332,"betaUser":false,"asusDevice":true,"localeIdentifier":"en-US","timeZone":"Asia\\/Calcutta","IMEI":"357996060367586","appIdentifier":"com.asus.userfeedback","appName":"ZenFone Care","appVersion":"2.1.1.66_160704"}'

You can also perform this experiment for your privacy issues :-
Using **Packet Capture** android application .



## Steps we can take to prevent our Privacy :-

### 1. Ultimate Privacy

Stop any android , apple and blackberry phone . Go for non smart phone or use ubuntu smart phones .

2.  Use mobile antivirus to block advertisement network or Root your phone and use iptables to control your traffic .

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-SSH  tcp  --  anywhere             anywhere           tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere           state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere           state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere           tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere           tcp dpt:ftp-data
REJECT     all  --  anywhere             anywhere           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-SSH (1 references)
target     prot opt source               destination
DROP       all  --  192.168.0.102        anywhere
RETURN     all  --  anywhere             anywhere
```