FAQ

Edit New Page

robo-mo edited this page 17 days ago · 102 revisions

Frequently Asked Questions (FAQ)

⚠️ This FAQ is designed to answer the most common questions. Please take your ⌚ to read it before you ask anything. ⚠️

Index

Quick Guide

Using AFWall+ the first time

1. Click on *Mode* to switch between whitelist- (default enabled) and blacklist-mode.
2. Mark the applications that you want to block or allow (depending on the selected mode), for each interface.
3. Open the menu and enable the firewall (green shield means enabled). If AFWall+ is already enabled, just select *Apply* and it will submit your changes.
4. The rules will be saved and automatically and restored when you restart your device. If not check the "data leak" option.
5. If you want to check all current IPTables rules, select *Firewall Rules* in the menu.

Widget(s)

To quickly enable or disable the firewall, add the AFWall+ widget to your home screen. There is no Widget description, the green shield means that the firewall is running, red means it's disabled. AFWall+ comes with three widgets, an settings widget, and two to toggle the firewall between enabled/disabled with profile(s) support and some basic options.

Firewall logs

If you want to see which applications have been blocked via AFWall+, open the menu and enable 'Log'. AFWall+ will then log each application blocked. You can check the log by opening the menu and selecting *More* -> *Show log*.

Password lock/unlock

You can set a password lock for AFWall+ by using the set *password* menu option. To remove the password protection, just reset it to blank (enter none).

Frequently asked questions

(1) What is IPTables?

> Please take a look here for a detailed overview.

Pages 28

Find a Page...

Home
Advertisements blocking
Android kernel traffic
Apps leak private user data during boot
BusyBox
Contributors
CustomScripts
DNS
Error codes
FAQ
Google Play services and other special cases
HOWTO blocking WhatsApp
HOWTO Compile AFWall
HOWTO Compiling busybox
HOWTO Compiling iptables

Show 13 more pages...

Clone this wiki locally

https://github.com/ukanth/a

Clone in Desktop

(2) How do I know if my device supports IPTables?

> Use the following command in ADB shell or in Terminal Emulator as root (`su`):

`iptables -h`

It doesn't matter in which folder iptables are stored (/system/bin/ or /system/xbin/) als long they have the correct ownership and permissions 755:root:shell (-rwxr-xr-x). To check on which place IPTables are stored simply use:

```
which iptables
which ip6tables

# They're normally under:
/system/bin/iptables
/system/bin/ip6tables

# or
/system/sbin/iptables
/system/sbin/ip6tables
```

(3) Packet processing in IPTables

> All packets inspected by IPTables pass through a sequence of built-in tables (queues) for processing. Each of these queues is dedicated to a particular type of packet activity and is controlled by an associated packet transformation/filtering chain.

- Forward (FORWARD) chain: Filters packets to servers protected by the firewall.
- Input (INPUT) chain: Filters packets destined for the firewall.
- Output (OUTPUT) chain: Filters packets originating from the firewall.
- Pre-routing (PREROUTING) chain: Address translation occurs before routing. Facilitates the transformation of the destination IP address to be compatible with the firewall's routing table.
- Postrouting (POSTROUTING) chain: Address translation occurs after routing. This implies that there was no need to modify the destination IP address of the packet as in pre-routing.
- Output (OUTPUT) via nat: Network address translation for packets generated by the firewall.

(4) Is a reboot required after edit/save IPTables?

> Changes to IPTables take effect immediately when they are run. If you are making your changes in a script, you must make sure that script gets run in order for the changes to take affect. The rules are enforced as soon as the actual commands are sent to the kernel. You will need to figure out how to run the script or apply whatever .conf changes you have saved to a file. A reboot actually clears all IPTables rules. On first boot the tables will always be empty, you always have to set all the rules after booting. That's what the AFWall+ automatically does (make sure it's enabled).

(5) How long does it take for an IPTables rule to apply?

> IPTables rules take effect immediately. Because your script is appending (-A) to the INPUT and OUTPUT chains, your rules are being added to the end of those chains. If you have other terminating rules that precede these rules, then they will take effect (and later rules will not). The only exception is that if the Kernel is busy with other network processing stuff.

(6) What is Active Rules?

> AFWall+ doesn't have control over IPTables itself. Any root/system application with access to IPTables can modify the rules. That's the reason, some time people gets app data leaks because some other process might have overwritten the OUTPUT chain to allow itself. To prevent this, AFWall+ will apply rules on every connectivity change.

> Also for roaming/LAN, AFWall+ need to change the IPTables rules in order to check Roaming status and LAN IP address.

(7) YouTube/Online Radio streaming is not working anymore. How can i fix this without disabling AFWall+?

> Please whitelist (allow) "Media Server" or remove it from your blacklist. Some Audio/Video apps may need such service.

(8) What does the little icons on top of the application(s) list stand for?

> From left to the right the icons meaning the following:

> **LAN** = All internal Local Area Network (LAN) traffic (default disabled, needs to be enabled in the options)

> **WIFI** = All traffic that goes through the wlan0 interface

> **Mobile** = All traffic that comes in/out from 2G/3G/4G/5G

> **Roaming** = Global roaming traffic which coasts money dependency on which provider you are connected to (default disabled, needs to be enabled in the options)

> **VPN** = All Virtual Private Network traffic e.g. from the Tor Network, OpenVPN or other providers (default disabled, needs to be enabled in the options)

(9) My logs (logcat) are not displaying anything or are always empty, why?

> AFWall+ logs are depend on dmesg (kernel logs). Either your kernel disabled dmesg or it's getting overwritten quickly. Please check if you kernel does have an option like "Android logger Control" or something like that an enable this service.

(10) Does AFWall+ support Android 4.4.4 or higher?

> Yes!

- UID 0 (root) needs 53/UDP open for DNS on Android 4.3. - Enable DNS/DHCP from within the application(s) list!
- UID 1000 (system) needs 123/udp open for NTP. - Enable NTP from application list!
- Android L/M may need a little configuration change and an external BusyBox app to get the rules apply. Try to experiment with the binaries option.

(11) Can I block incoming SMS/MMS? - Premium SMS?

> Android OS (5+) includes support for warning users of any outgoing premium SMS message. Premium SMS messages are text messages sent to a service registered with a carrier that may incur a charge to the user. Device implementations that declare support for *android.hardware.telephony* MUST warn users before sending a SMS message to numbers identified by regular expressions defined in `/data/misc/sms/codes.xml` file in the device. The upstream Android Open Source Project provides an implementation that satisfies this requirement. See here for more information.

(12) Can I block IPv6 traffic?

> Sure, please use AFWall+ 1.2.4 (or higher). Some kernels have an option to disable IPv6, make sure it's enabled (reboot required). *Enable IPv6 support* in AFWall+ options because this is disabled by default. Take also a closer look about the important notes from IPv6 over here.

> If you use custom scripts this option could be problematic in some cases, uncheck it if you script returns an error message.

(13) Is there Tasker/Locale support?

> Tasker/Locale apps working together with AFWall+ (1.0.4a or higher).

(14) UDP Port 53 (DNS) is blocked if whitelisting mode is enabled, why?

> Please read this and the DNS Wiki article. It's **disabled by default on whitelist mode**. Enable DNS/DHCP from the application(s) list will unlock it.

(15) How can I show actually used IPTables rules?

> Via *iptables -L* command in apps like Android Terminal Emulator. Most ROMs comes already with this.

Or

> Via `Firewall rules` from the AFWall+ preferences.

(16) Can my apps bypass AFWall+ whitelist mode before the boot is complete?

> Please read this.

> If you want to see what is connecting during the boot take a look at the */proc/uid_stat/* folder.

Important note: procfs is mounted at boot time, which means that every time your device is getting rebooted there are 0 traffic values for all UIDs. You can list */proc/uid_stat/* dir right now to see which UIDs have been spending traffic since last reboot.

(17) How do I display all available network interfaces names using bash shell prompt?

> Open Android Terminal Emulator and type this:

```
$ ip link show
```

> Each network interface config is stored under the `/sys/class/net/` dir. If you list that dir on Android, you'll probably see something like that:

```
$ ls sys/class/net
lo
dummy0
ifb0
ifb1
rmnet0
rmnet1
rmnet2
usb0
sit0
ip6tnl0
gannet0
tun
eth0
```

(18) How can I purge IPTables rules?

> Open adb shell or Android Terminal Emulator and type this:

```
su
iptables -F
iptables -X
Reboot
```

> You can also do this via `Firewall Rules` option and click on the `flush rules` button.

(19) AFWall+ does not show app xyz in my list, why?

> Only apps are listed that have **internet permissions** in the AndroidManifest.xml. If it's not listed this means that this app don't use any internet permission.

(20) AFWall+ does not work under CM 7.x - 12.x. How can I fix this?

> CM 7.x uses an old version of IPTables which has maybe conflicts with AFWall+ own built-in IPTables. As a workaround you can try to update your IPTables to the latest version. But it should work without it. CM 11 users may need to change the BusyBox version from *builtin* to *system BusyBox*. Of course you need to install it first.

(21) How to install AFWall+ as a regular app?

> Just download it via F-Droid, Google Play Store, or here on GitHub. Then install it. That's it!

> Advance users can directly install it via adb:

`adb install afwall+.apk` (default install method)

> Or you may also copy and download the afwall+.apk file on your device and install it using any file explorer.

(22) How to install AFWall+ as system app (only for test reasons!)

```
adb remount
adb push afwall+.apk /system/app (or /system/priv-app/ Android 4.3 or higher)
```

> You may also move the .APK file to the */system/app* directory manually. Make sure you set the file permission properly *-rw-r--r--*. To uninstall, please remove afwall+.apk from */system/app* manually.

(23) Which permissions are used?

> - *RECEIVE_BOOT_COMPLETED*: Autostart (Bootup) AFWall+ after the system finishes booting.

- *ACCESS_NETWORK_STATE*: Allows AFWall+ to access information about networks (IPTables).
- *WRITE_EXTERNAL_STORAGE*: Allows AFWall+ to write to external storage for debug log and export IPTables rules.
- *ACCESS_SUPERUSER*: Standard to support Superuser (by Koushik).
- *INTERNET* : NetworkInterface.getNetworkInterfaces() needs android.permission.INTERNET. This is just being used to get the IPv4 and IPv6 addresses/subnets for each interface, so the LAN address ranges can be determined. Nothing is actually trying to access the network.
- *ACCESS_WIFI_STATE* : Added to detect tether state.

(24) How can I disable the firewall temporarily?

> If you need to disable the firewall temporarily, you can flush all the rules by using

`iptables -F`

Or via an external script:

```
echo "Stopping the firewall and allow everything..."
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -t raw -F
iptables -t raw -X
```

```
iptables -t security -F
iptables -t security -X
# Apply and allow now your rules from here ...
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

Or within AFWall+ itself, via the available widget(s).

(25) Can you help me with rooting my device?

> There are already enough guides to help you to root your device. Use your favorite search engine to find one.

(26) Does AFWall+ needs a lot of battery/memory?

> Not really. Usually around *11 - 16 MB* (non shared memory), dependent which configuration you use. It also does not use many CPU cycles (which is a good an indicator that it does not waste battery energy).

(27) How safe is AFWall+?

> Nothing is really secure, see the limitations in the README.md for more details, but it's better to install a Firewall and control the incoming/outgoing packages than have nothing installed. If the app may crash sometimes than feel free to submit a error log report via eMail or here on our GitHub Issue tracker, we are always motivated to fix problems and answer your questions as soon as possible.

(28) How can I make a logcat to indicate what caused the crash?

> Please take a deeper look at our Howto report a bug + HOWTO debugging articles for additional help.

(29) Will there be an iOS or Windows version?

> No, because it's too difficult to implement something like AFWall+ on those systems since they are not open source and/or do not support netfilters.

(30) Does AFWall+ work with SELinux (aka Fort Knox)?

> It should work without any big problem. For more info please look here and here.

> To toggle between enforcing and permissive mode just use adb

```
# 1 = enforcing mode / 0 = permissive
adb shell su 0 setenforce 1
# On an emulator simply use
emulator -selinux permissive
```

(31) Can AFWall+ be detected by other applications?

> Yes, but it should be no security problem as long as the rules not get touched.

(32) Do I need to have the Google Play Store installed for the donate version?

> No! There is no hidden license check integrated. There is also no "call home" function.

(33) What happens if I make AFWall+ device administrator?

> Android includes features that allow security-aware applications to perform device administration functions at the system level, such as enforcing password policies or performing remote wipe, through the Android Device Administration API. This ensures that other applications cannot uninstall AFWall+ without your knowledge. Device implementations must provide an implementation of the *DevicePolicyManager* class. Device implementations that include support for lock screen must support the full range of device administration policies defined in the Android SDK documentation and report the platform feature *android.software.device_admin*.

(34) Why does the Kernel need an internet connection all the time? AFWall+ shows AppID (-11) blocked.

> The kernel does not communicate directly, it only pass packet information (for the interfaces e.g. uid0) from some applications. One problem with using policy routing based on fwmark with locally generated traffic (as is the case with Android) is that the mark must be set in the user process. It is because the routing decision is made before the fwmark can be set in any iptables rule, at least in vanilla kernels.

> Since Android 4.3 and higher all DNS requests are manged by the netd daemon, it works similar like an proxy/tunnel. That means AFWall+ can't detect the special UID's / DNS requests. To disable such behavior you can use the *DNS-Proxy* option under *Preferences*. Choose *Disable DNS via netd* to restore the default behavior before 4.3. Now you should make sure that your apps are whitelisted, if not it will be blocked, same with your (Root) application, if not Android is maybe not able to establish a connection. Dnsproxy2, is an alternative app to redirect DNS requests. But if there are troubles with your connection, check your logs, use Netzwerk Log app (identify all traffic), whitelist the specific app(s) that is maybe blocked or enable the netd daemon again.

(35) Why was my issue closed on GitHub?

> Things like ***It doesn't work*** or ***it crashes*** **are insufficient**. Please describe the exact steps to reproduce the problem and always provide a logcat. More info always means that we can better help you.

> It's also possible your issue is a duplicate, or is already fixed. Please watch the Changelog.md and TODO.md files carefully.

(36) Does AFWall+ support nftables?

> No, AFWall+ does not support nftables yet. There is currently no Android nftables firewall available on the entire www.

(37) Can I use XPrivacy, Lightning Wall, or any other Firewalls/Security apps together with AFWall+?

> - XPrivacy: Will work fine with AFWall+ as long as you do not restrict any AFWall+ in any way that will prevent it from working (do not block its internet access or system-related functions like 'IPC'). If there is any problem you can watch what is blocked under the *Data Usage* section in XPrivacy and try to remove it.

- Lightning Wall: Works fine together with AFWall+, because it does not interact with IPTables (leave IPTables unchecked).
- Avast: please disable this firewall if it's turned on (unchecked by default).
- Android Tuner: Same as Avast, but the Firewall is disabled by default.
- DonkeyGuard: It can't control IPTables, but Android's permission, so generally it work but don't restrict some important functions like *write_external_storage*, or AFWall+ log can't be created on your sdcard.
- OrWall: OrWall is not compatible with AFWall+. Please disable it and enable the *Transparent Proxy* option in Orbot.

- Adblock Plus: Comes with their own IPTables, but it should be no problem to use it together with AFWall+. If something went wrong and you like to report a bug, please disabled it first and try to reproduce the problem, if you manually created/enabled a proxy, shut it down first.
- An overview of similar solutions is available over here.

> Generally it is not necessary to use two firewalls together and it could be problematic if you don't know what you are doing. 🎱

(38) Will you integrate a HOSTS blocking option?

> No (see #285 & [#223] (https://github.com/ukanth/afwall/issues/223)), AFWall+ is a firewall and not a all-in-one solution for all "security" related problems on Android. The goal is to control IPTables with some gimmicks such as custom scripts - which is already implemented. A big hosts file can also slow-down non high-end smartphones, block some ads which some developer need to get money and can block some sites you may need. There are also other solutions to handle it, like MoaAB or and Xposed module called UnbelovedHosts. For additional question take a look over here.

(39) Can I ask about *xyz* that was not explained here?

> If you have any questions, please create a post in the XDA AFWall+ forum thread.

If possible please do not ask questions using GitHub issues! GitHub issues are designed for bug reports and feature requests.

(40) Is there a BusyBox solution that does not need root?

> Yes, there is a solution coded by Jared Burrows, but it doesn't provide all extra binaries, the most common used are included in this package. Visit this page for more information, or get it directly from Google Play Store. We not recommend to use it due several problems that package might contains.

(41) What does UID mean?

> The Android OS is based on Linux, so basically it is the same UID you have in a Unix-like OS. When installing an app/package, Android by default creates a UID specifically for that package, so that it can have its private resources/storage space. When no packages are using anymore that UID (which could be shared), the UID is deleted.

> We can override this behavior with android:sharedUserId, but it has some drawbacks.

(42) How to change the DNS settings under Android? (optional, normally not necessary)

> Please read this article to answer most DNS related questions. By default the Google DNS servers will be used.

(43) Will there a "Connection confirm dialog" (on-demand) feature implemented soon?

> It's already been asked #269, there is currently *no* Android firewall which include such feature yet. There is also no on-demand firewall based on IPTables available on Google Play Store or F-Droid.

(44) Will you implement an AdBlock function, and why are some Ads are still visible if I try to block them via IPTables?

> First of all, AFWall+ is not an Ad-blocker! It's a firewall, which is not able (and never will be) to block all your visible ads and there are some good reason. Some app developer make money with in-app advertising (ie AdMob) and if we block this, no one is motivated to make some awesome apps anymore. If you really want to block such ads, you still can use MinMinGuard, but it's general a bad idea to block all things. For a quick overview over ad blocking please take a look at the Wikipedia article.

> I blocked ads with ad server hostnames and IP addresses. Why they are still visible?

> There are some limitations e.g. Adblock Plus for Android does not allow ads to be blocked on https/SSL encrypted websites [due Android limitations], some ad-servers use a proxy behind it, and it's generally hard to filter JavaScript generated content, currently there is no element hiding addon for Android. The easiest way is to block ads on Android is to manipulate your DNS/Hosts file, for this you can use this or this Hosts file which getting regular updates. There are some alternative ways, but on newer Android systems they not seems to work anymore due some internal changes.

> And why was Adblock Plus removed from Google Play Store?

> Read the full story here.

(45) I don't have the IPTables binary on my device, what can I do?

> If you have netfilter enabled in your kernel and not have the IPTables binary you can use the AFWall+ in-build IPTables (make sure you enabled it in the options).

(46) Is there a good app to collect basic Network Info?

> AFWall+ already collects some useful information in the *Firewall Rules* dialog but if you need a good and free alternative tool to show some more information use e.g. Network Info II.

(47) The startup-script is still present how can I remove it?

> In the normal case, AFWall+ should automatically check/detect if you have the *afwallstart* script in the init.d dir. A simply press of *Fix Startup Data Leak* should remove/re-enable it again, but in a rare situation the system needs to be remounted again. In this case, you can remove the script with your favorite file explorer app under `/system/etc/init.d/afwallstart` or via ADB/Terminal.

```
su
mount -o remount,rw /system
rm -f /system/etc/init.d/afwallstart
mount -o remount,ro /system
reboot
```

(48) How can my script survive an Over-the-Air (OTA) Update?

> Just navigate to /system/addon.d/ and copy the `50-cm.sh` file. You can rename the copy to whatever you want for example 98-myfiles.sh, now open it and search for the line etc/hosts and add the script you want to protect in our case we want to protect the afwallstart script (present if you use the experimental fix data leak option in AFWall+):

```
...
. /tmp/backuptool.functions

list_files() {
cat << EOF
etc/init.d/afwallstart
etc/gps.conf
EOF
}

case "$1" in
  backup)
    list_files | while read FILE DUMMY; do
      backup_file $S/"$FILE"
    done
  ;;
  restore)
    list_files | while read FILE REPLACEMENT; do
```

```
      R=""
      [ -n "$REPLACEMENT" ] && R="$S/$REPLACEMENT"
      [ -f "$C/$S/$FILE" ] && restore_file $S/"$FILE" "$R"
    done
  ;;
  pre-backup)
    # Stub
  ;;
  post-backup)
    # Stub
  ;;
  pre-restore)
    # Stub
  ;;
  post-restore)
    # Stub
  ;;
chmod 0755 etc/init.d/afwallstart
chown root:shell etc/init.d/afwallstart
chcon u:object_r:zygote_exec:s0 etc/init.d/afwallstart
esac
...
```

> The last step is to save the file and set the correct permission. (root:root -rwxr-xr-x bzw. 755)

(49) How can my script survive a system wipe?

> This is a little bit harder but not impossible. It's almost the same procedure as mentioned in FAQ48 except the dir you need to place the file in; /data/local/userinit.d/ (if not present just create it - root:root -rwxr-xr-x bzw. 755) Now place your script in there. To restore other script just put it under /data/local/.

```
#!/system/bin/sh
# This is the script /data/local/userinit.d/98-afwallstart-repair
# (permissions root:root -rwxr-xr-x 755)
# It takes care, that the AFWall+ firewall is correctly blocking network
# traffic at boot time (see data leak fix)

# We want to write to the system partition
mount -o remount,rw /system

# Take care that (OTA) updates do not break AFWall's firewall security
cp /data/local/afwallstart /system/etc/init.d/afwallstart
chown root:root /system/etc/init.d/afwallstart
chmod 555 /system/etc/init.d/afwallstart

# Take care that system wipes do not harm our tweaks
# as example we use the script file name "98-myfiles.sh"
# for this, uncomment the following 3 lines = remove the "#"
#cp /data/local/98-myfiles.sh /system/addon.d/98-myfiles.sh
#chown root:root /system/addon.d/98-myfiles.sh
#chmod 755 /system/addon.d/98-myfiles.sh

# lock up system partition read-only
mount -o remount,ro /system
```

(50) Where are AFWall's settings stored?

> Exported content like profiles are stored under your internal sdcard /sdcard0/afwall all other stuff is stored under /data/data/dec.ukanth.ufirewall/.

(51) I get "Unable to parse package." if I try to install AFWall+, what can I do?

> This means AFWall's .apk file seems to be corrupt. Try disabling your popup-/ad-blocker, re-check your internet connection and re-download the apk.

(52) I use Opera Max as my browser with "Turbo Mode" enabled. Why does adblocking/firewalls seem to not work anymore?

> For debugging and error reporting just disable the "Turbo Mode" option, this is mostly only another term for VPN/Proxy which works behind this option. No Firewall, IPTables, Proxy or any external app works with this option enabled, since it's not possible to use two VPNs the same time (i.e. local/inet). It's not possible for any app to look behind this traffic (local). Other Browser may have a similar function or add-ons (like Firefox Janus-Proxy or Chrome's bandwidth safer feature), ensure it's disabled.

(53) Since AFWall+ 2.x I don't see any reload applications button

> This was removed, just touch on the main screen and swipe down, this feature is called swipe to pull.

(54) How can I sort the application(s) view in the main screen?

> Under 'Preferences -> Experimental Preferences' there is the *Sort Application* option that allows you to sort your apps via 'Name (default enabled)', by 'Install/Upgrade time' or by the app's UID.

(55) What's the difference between AFWall+ Unlocker and AFWall+ Donate?

AFWall+ Free - Free version of AFWall+ AFWall+ Donate - Donate version of AFWall+ AFWall+ Unlocker - Unlock donate features in AFWall+ Free version

Use Unlocker over Donate

1. Test AFWall+ Beta versions (usually updated first in AFWall+ Free version)
2. Supporting development by IAP
3. Works on multiple devices

AFWall Free + Unlocker == AFWall Donate

(56) Will AFWall+ work together with Android M 'verify boot' protection enabled?

> This must be disabled since it will break *SU*, it checks every start if the firmware was manipulated (STOCK). An solution would be to disable it within the ROM or switch to another ROM like CM which will get an option to take control over it. See also, Chainfire's statement about the future of SU.

(57) I use Android 5/6 and 'Privacy Guard' shows me SMS and other permissions, why AFWall+ requests for it?

> Privacy Guard isn't enabled by default and claims to 'secure' the OS a little bit more, in fact for beginners it can be a bit confusing if you enabled it, because the information which permission the app uses (in our case AFWall+) are 'wrong', means it shows common dangerous permissions that can/could compromise your security (like composing/sending SMS, share/access your location and other things). If the app is not explicitly designed to fit with privacy guard rules you possibly will see the mentioned 'wrong' permissions. In fact, AFWall+ never ever requests for any of them, if you used any version which isn't original and you see that SMS will be send or something like that, this mostly means you use an infected/faked app!

(58) What do I need to do to get Google Play Store to work?

> You need to whitelist the following: com.google.android.gms (Google Play Services for authorization) + com.android.providers.downloads (For Downloads) + com.android.vending (this is the Play Store).

(59) After using AFWall+ I constantly see a '#' symbol in the notification bar, how can I remove this?

> This starts with CM/12/13/Android 5.1.1/6 which original was designed to add an indicator for applications which requiring root permission so this is not only AFWall+ related. You have three options: ignore the symbol, install chainfire's SuperSU or install Xposed with an module to hide this icon. Please also read this and this.

(60) I want use AFWall+/NetGuard with AdGuard together how can I do this?

> AdGuard uses the Android VPN API which is the same API required for NetGuard. Android does not allow two VPN's to be used together at the same time, so you need to set the http-proxy in AdGuard. On AFWall+ you only need to disable AdGuard's integrated firewall. Optionally, you can add exclusions in the low level setting to exclude dev.ukanth.ufirewall and eu.faircode.netguard so that the apps aren't filtered by AdGuard (not necessary, but can possibly avoid some problems), since both AFWall+ and NetGuard are not integrating ads, it is recommended to add this.

(61) What is Android's Captive Portal Check?

> Each time you connect to your WLAN Access Point, Android tries to check if you're not only connected with it, it wants to do a check which ensures that there are really targets available. Usually a Captive Portal Check makes sense whenever you're in a hotel or airport because in such a case you get a code/coupon to login into the WLAN, this acts like a activation/authentification process. Android tries to send the packages over 'http://clients3.google.com' and if the answer is susessfully you get an HTTP Response-Code 204 (the answer is correct but it doesn't contain any data). Basically the IP and a timestamp will be transmitted. To change this behaviour you can use:

```
//Android 4+
settings put global captive_portal_detection_enabled 0
settings put global captive_portal_server localhost

//Since Android 7
settings put global captive_portal_mode 0
```

You can also refer Issue-761 for more details

--END--