1. Rule

1.1 What are rules

Those who are familiar with firewalls and route tables must know these two things are basically defined by rules you pass to them. Take a firewall as example, it must explicitly know which destination hosts are allowed, or which ports are forbidden, in order to function properly. In the same way, a router must know which next hop to send the current packet based on the destination IP address.

For Postern, rules play similar roles. Generally speaking, Postern manages all out-going traffic from your device. That means, when an APP initiates a new access request(a TCP connection), Postern will have to make a choice from below options:

1. To block the request
2. To direct the request and all subsequent data through a proxy server
3. To let the request and all subsequent data go directly to its destination

Basically Postern will choose one from above three options when it sees a connection and its data, based on the rules you pass in. For example, some APPs visit certain sites to fetch Ads. You might want to tell Postern to block these access attempts by a rule. Another example is you want to hide your IP address when visiting certain sites, then you might want to add a rule that tells Postern to direct traffic to these sites through your proxy server.

In a word, rules play most important rules. Postern manages all traffic your device entirely based on the rules on configure.

1.2 How rules are configured

Postern recognizes and takes in a text-format configuration file. The format itself is easy enough to be self-explained. This guide won’t go so far as to explain every detail of configuration file format. The examples we use below will tell you everything you need to know to write your own configuration file.

The first to explain is how Postern matches a destination address to a rule. Yes, like route tables, Postern looks for a rule using destination addresses of data packets. To explain this further - When it sees data traffic to a certain destination address, it uses this address to lookup in the rule set, in an attempt to find a matching rule, and see what action this rule specifies. And usually, an address has two different layers of meaning – a domain name and an IP address. For example, in order to visit www.google.com, your web browser has to resolve this domain name to an IP address. The IP address and 'www.google.com' both point to the host that contains the web contents you request. Consequently, Postern has two catagories of matching methods:

1. Domain-Name-based method group, which contains 3 different types of method:

1.1. Match domain keyword (DOMAIN-KEYWORD)
When the rule-specified string matches any of the domain's sub string, the rule is considered a match.
Eg: *DOMAIN-KEYWORD,google,REJECT*
www.google.com, www.google.com.cn will match this rule, meaning anything access attempts to these sites will be rejected. But www.googleusercontent.com won't match this rule.

1.2. Match domain suffix (DOMAIN-SUFFIX)
When the rule-specified string is the domain's suffix, the rule is considered a match.
Eg: *DOMAIN-SUFFIX, google.com, Proxy*
www.google.com, mail.google.com will match this rule and all traffic to these sites will go through your proxy named 'Proxy'. In the meantime, www.google.com.hk will not match this rule.

1.3. Perfect Match domain (DOMAIN)
Only when the rule-specified string perfectly matches the domain name, will the rule be considered a match.
Eg: *DOMAIN, www.google.com ,Proxy*
Only www.google.com matches this rule and all traffic to this site will go through your proxy named 'Proxy'.
mail.google.com, www.google.com.cn will not match this rule.

2. IP-address-based method group, which contains 2 different types of method:

2.1. Match an IP address's country

When the IP address's country matches the one specified in the rule, the rule is considered a match.
Eg: *GEOIP, US, DIRECT*
You access to any US-based servers with a public IP address will match this rule. Eg, an attempt to access www.google.com (216.58.216.4), will match this rule.

The GEO-IP database of Postern contains IP information of 236 countries. This guide will provide a list of these countries and their country codes.

2.2. Match an IP address's CIDR
A rule defines a IP subnet; When an IP address matches this subnet, the rule is considered a match.
Eg: *IP-CIDR, 192.168.0.0/16, DIRECT*
All access to 192.168.1.10, 192.168.100.1 matches this rule.

Another match method is defined to match any addresses:

3. Match all
For any domain names or IP addresses, the rule is considered a match.
Eg: *FINAL, DIRECT*
This rule usually comes last in a rule set (hence the name). That means when Postern has failed to find a rule for access to a certain destination, this rule will be the final match.

You might have noticed all rule examples above comprise of 3 parts, delimited by commas. The first part defines the matching method – any of the 6 illustrated above. The second part defines how the rule is to be matched. The last part, which is explained below, defines the action Postern takes when it considers this rule a match. There are five different actions currently supported:

1. **Direct** – For connection attempts and subsequent data that match this rule, forward them directly to destination host

2. **Proxy** - For connection attempts and subsequent data that match this rule, let them go through the specified proxy server

3. **Block** - For connection attempts and subsequent data that match this rule, drop them all

4. **Smart Select** – For connection attempts and subsequent data that match this rule, try using 'Direct' action first; If that fails, use the specified proxy server instead.

5. **Proxy Group** – A proxy group is a combination of different options. Users can decide which of these options to use at run-time. For connection attempts and subsequent data that match this rule, user's most recent choice will be used for them. Proxy Group will be explained in detail in a later section.

For rules that use action 2 (Proxy) and 4 (Smart Select), a proxy server must be defined along with the rule. Proxy servers are defined by names.

For rules that use action 5 (Proxy Group), a proxy group name must be defined along with the rule. Proxy groups are defined by names.

Currently the configuration file supports all actions above except action 4 (smart select). You still can configure a rule's action to 'Smart Select' on UI.
In a configuration file, the 'action' field of each rule can be:

1. **REJECT** – means action 3 (Block)
2. **DIRECT** – means action 1 (Direct)
3. **Proxy name or Proxy Group name** – specifies the name of the proxy server or proxy group. Postern searches this name in the [Proxy] section or the [Proxy Group] section of the configuration file. If a match is found in the [Proxy] section, the action of this rule is action 2 (Proxy). If a match is found in the [Proxy Group] section, the action of this rule is action 5 (Proxy Group). If no match is found in either section, this rule will be ignored by Postern.

1.3 Odering of Rules

Those of you who have dealt with route tables must know a thing or two about ordering. A destination usually can match more than one rule in a rule set. In such cases, the first matched rule is used. An example is as blow:

```
[Rule]
DOMAIN-KEYWORD, google, DIRECT
DOMAIN-SUFFIX, google.com, REJECT
DOMAIN, www.google.com, Proxy
```

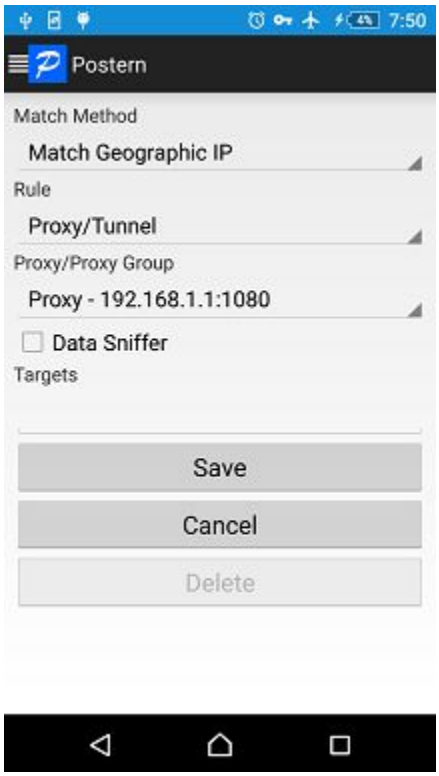
When your browser initiates a new connection to www.google.com, all three rules may apply. And they are telling Postern to do different things. In cases like this, Postern always chooses the first rule that it finds is a match. In this case, Postern lets your browser access www.google.com directy.

1.4 Configuring rules on UI

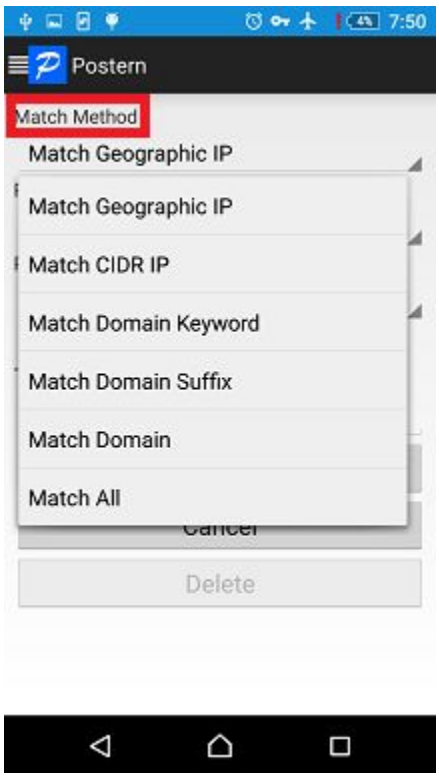
Postern allows you to directly configuring rules on its graphic user interface, as well as importing a rule set from configuration file. In this way, you can also make further adjustment after importing a file.

Adding Rules

Click 'Rules' from the navigation panel on the left. You'll see the panel above. Click 'Add Rule', as below:

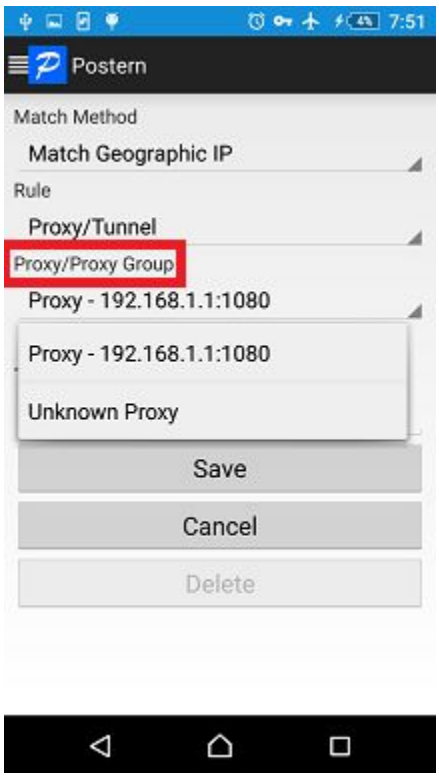


In 'Match Method', select a method you would like Postern to use to match destination address against this rule. As discussed above, there are 6 different methods in total available.



In ‘Rule’, select the action you would like Postern to take when it finds this rule a match. As discussed above, there are 5 options here, as below:

If ‘Proxy/Tunnel’ or ‘Smart Select’ is what you choose here, you’ll also need to designate a proxy server in the ‘Proxy/Proxy Group’ combo box.



If you choose ‘Proxy Group’, you’ll need to designate a proxy group in the ‘Proxy/Proxy Group’ combo box.

In the ‘Targets’ section, write down the contents of your rules, delimiting them with ‘;’. These things here correspond to second parts of ‘,’delimited rules. For example, you have rules in your configuration files as below:

```
[Rule]
DOMAIN-SUFFIX, google.com, Proxy
DOMAIN-SUFFIX, twitter.com, Proxy
```

You’ll need to write down ‘google.com; twitter.com’ in the ‘Targets’ section, as below.

The effect of this rule is, all access/traffic to domain names that end with google.com or twitter.com, will go through your proxy server 192.168.1.1:1080. The configuration file equivalent is as below.

```
[Proxy]
Proxy = https, 192.168.1.1, 1080, username, password

[Rule]
DOMAIN-SUFFIX, google.com, Proxy
DOMAIN-SUFFIX, twitter.com, Proxy
```

Edit/Delete Rules

In the same way of adding a rule, you can edit an existing rule by clicking it, and delete it from your rule set by clicking the 'Delete' button.

Inserting Rules

It's worth mentioning again the ordering of rules in Postern. Postern always chooses the first rule that is considered a match. So you may want to insert a new rule after or before an existing one.

Long press an existing rule, a popup menu will show up. Click 'Insert new rule before', and a new rule will be inserted before that one(After you complete editing and save it, of course). Alternatively, click 'Insert new rule after', and a new rule will be inserted after that one. Click 'Delete', the selected rule will be deleted.

2. Proxy Server

Actually we have shown you how a proxy server is defined in configuration file, in examples above. Proxy servers are grouped together and defined in the [Proxy] section, as below.

```
[Proxy]
Proxy = shadowsocks, 11.22.33.44, 1080, aes-256-cfb, password
Proxy2 = ssh, 22.33.44.55, 22, username, password
```

Two different proxy servers are defined, named 'Proxy' and 'Proxy2' respectively. Their names are referenced in the [Rule] section. On the right side of '=', from left to right, the type of the server, server's address, server's port, username and password are specified.

It should be noted names of proxy servers must contain alphabetic characters, digits and underscores only.

Some more details about the various fields required to define a proxy server(stuff that are on the right side of '=')

1. **Type of Proxy server**

Currently up to 5 different types of proxy servers are supported:

SSH – SSH tunnel (RFC 4254)
SOCKS5 – The standard SOCKS5 tunnel (RFC 1928)
HTPP CONNECT – The standard HTTP CONNECT method (RFC 2817)
Shadowsocks – A popular encrypted tunneling method invented in China
GFW.PRESS – An encrypted tunneling method invented in China

2. Proxy Server Address

This field can be an IP address or domain name of your proxy server. In the example above, 'Proxy2' is an SSH server at 22.33.44.55

3. Proxy Server Port

Thiw field is the port number of your proxy server.

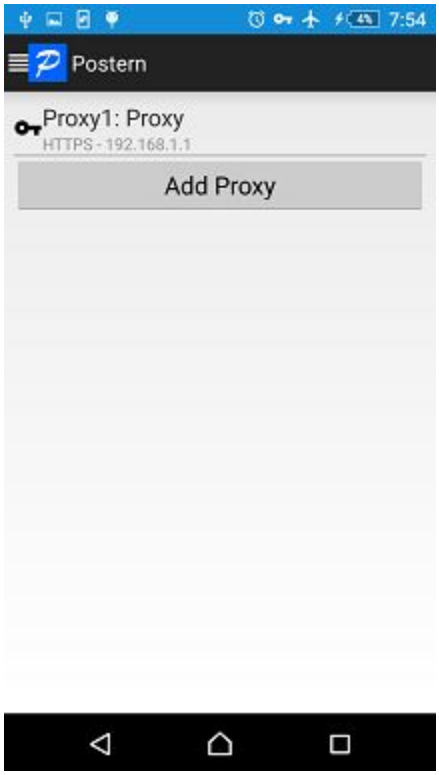
4. Username/Encryption for Shadowsocks

Username to login to your proxy server. For Shadowsocks protocol, no username is needed so this field is the encryption used on the proxy server. Please refer to Shadowsocks protocol specifications (Mostly its source codes) for a list of encryption types.

5. Password

In conjunction with username to login to the server.

Let’s take a look at how proxy servers can be configured on UI. On the left-side navigation panel, click ‘Proxy’:



Click on an existing proxy server will leads you into its configuration panel. Click ‘Add Proxy’ and you’ll see the panel that asks for your proxy server information discussed above. The panel looks like below.

Put in your proxy server address, port, type, username and password/encryption. Below figure shows the supported proxy types.

3. Proxy Group

You may have many rules in your rule set, many of which point to the same proxy server. But somehow you would like different proxy servers when you are at home and having WIFI and when you are outside using carrier's data service. But it's much trouble that you maintain two different configuration files, or you manually change each rule when you switch between two different networks. Here's where proxy groups can play their roles. A proxy group corresponds to a list of different actions. When you change current selection of a proxy group, all rules that use this proxy group will switch to that new selection and use it as the new action.

An example is as below:

```
[Proxy]
Proxy_WIFI = SSH, 11.22.33.44, 22, username, password
Proxy_4G = Shadowsocks, 22.33.44.55, 8888,
aes-256-cfb,password

[Proxy Group]
ProxyG = select, Proxy_WIFI, Proxy_4G

[Rule]
DOMAIN-SUFFIX, google.com, ProxyG
DOMAIN-SUFFIX, twitter.com ProxyG
```

In the UI, there's a 'Proxy Group' in the left-side panel. There is a proxy group item named 'ProxyG', that has two options – Proxy_WIFI and Proxy_4G. You can switch between these two options and the rules will use relevant proxy servers accordingly.

It should be noted that Proxy_WIFI and Proxy_4G must both be properly defined in the [Proxy] section.

'REJECT' and 'DIRECT' can also be used as proxy group options. To do that, you define pseudo proxy servers in the [Proxy] section. Below is an example.

```
[Proxy]
Pseudo_REJECT = REJECT
Pseudo_DIRECT = DIRECT
MyProxy = https,1.2.3.4,443,username,password

[Proxy Group]
ProxyG = select, Pseudo_REJECT, Pseudo_DIRECT, MyProxy

[Rule]
```

```
DOMAIN,www.google.com,ProxyG
DOMAIN-SUFFIX, twitter, ProxyG
```

In the UI, you'll see three options under 'ProxyG' – REJECT, DIRECT and through proxy server 'MyProxy'. Again, choose one of them and all rules that use 'MyProxy' as their actions will change their action accordingly.

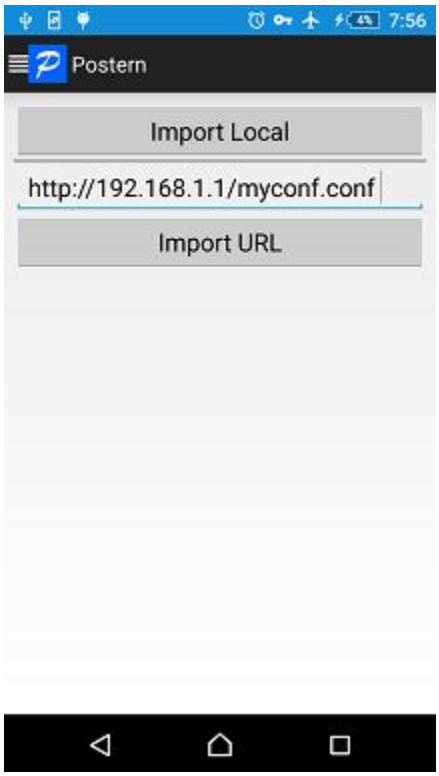
Below is what ProxyG looks like after you import above configuration file

It must be noted that each proxy group must begin with a 'select'.

4. Import Configurations

You've seen many examples of configuration files. Your touch screens and keyboard-less devices are usually not designed for such complex configurations. Hence Postern defines its configuration file and let you import them. After all, writing down these configurations on a computer with a keyboard before import them on your mobile device is much more convenient. A configuration file is text-based and thus is easy to read and propagate to your fellows.

To import a configuration, click 'Import Proxy/Rule' on the left-side panel. And below panel shows up.



You can download your configuration file from your computer to your mobile device. And click 'Import Local' to find it and import. Or you can put your file somewhere on the Internet and punch in the URL and click 'Import URL' to import.

For some more examples as to write your configuration file, here's a link to Postern related materials:

https://github.com/postern-overwal/postern-stuff

We'll update this site from time to time.

5. GEOIP Supported Country Codes

GEOIP allows you to distribute data traffic based on the geo-location they are going. For example, a proxy APP has a feature that puts traffic destined for foreign servers through a specified proxy server, but makes data to domestic go directly to their destination hosts.

The configuration file is as below:

```
[Proxy]
MyProxy=Shadowsocks,22.33.44.55, 8888, aes-256-cfb,password

[Rule]
GEOIP,CN,DIRECT
FINAL,MyProxy
```

There are two rules in total. The first one tells Postern to use direct connection when it sees an access attempt to a Chinese host. The other rule tells Postern to use proxy 'MyProxy' for all the rest of data.

If you happen to have multiple proxy servers residing in different countries, and you can use these proxy servers to accelerate your data traffic to these countries. A configuration for you is as below.

```
[Proxy]
HK_Proxy=Shadowsocks,22.33.44.55, 8888,aes-256-cfb,password
US_Proxy=SSH,1.2.3.4,22,username,password
JP_Proxy=HTTPS,2.3.4.5,1080,username,password
GB_Proxy=SOCKS5,5.6.7.8,10080,username,password

[Rules]
GEOIP,HK,HK_Proxy
GEOIP,US,US_Proxy
GEOIP,JP,JP_Proxy
GEOIP,GB,GB_Proxy
```

In this example, you have proxy servers in Hongkong, USA, Japan and Britain. For traffic destined for Hongkong, the proxy server in HK is used. Traffic destined for other countries are distributed to their corresponding proxy servers in the same way.

NOTE: Data distribution based on GEOIP rules depends largely on your DNS servers. If your DNS servers return incorrect IPs for certain domain names, you may not see expected outcome from your rules.

Postern now supports up to 236 countries and regions, as listed below. Each country or region is represented by a 2-character code. You may refer to https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2 for more details.

```
ZA EG ZW LR KE GH NG TZ
MU ZM MG AO NA CI SD CM
MW GA ML BJ TD BW LY CV
RW CG UG MZ GM LS MA DZ
GN CD SZ BF SO SL NE CF
TG SS BI GQ SC SN MR DJ
RE TN YT ST GW KM ET ER
AU CN JP TH IN MY KR SG
TW HK PH VN NZ BD PK ID
```

NP PG TK KH MO MV AF NC
FJ MN WF MM LA LK BN AE
NR NL GU VU BT WS FM PF
TL TO GB MP TR US NU SB
KI PW NF BS BZ VG CA MH
FR IR SE AS KP NO TV IO
CK KY PR BB VC JM BM DE
TC VI DM AG PM MF GD AI
MQ GP CZ FI CH IT BE BL
LC KN MS ES LU AT IL IE
DO MX AR TT CO VE BO BR
CR CL UY PY CW HN PA SV
SX PE EC GY GT NI BQ AW
HT CU GF SR EU RU KZ PT
GR SA DK SY UA CY IQ RO
LB GE AZ PS LT OM RS IS
HU BG SI MD MK EE LI HR
PL BA LV JO KG IM AM YE
BY GI SK MT QA AL JE SM
KW ME TJ UZ BH GL VA FO
GG MC AD TM