

Reverse_Proxy_with_apache_mod_proxy

So with public IPv4 addresses running out, when moving over to my new KVM hosting setup, I had to give a Private IP 192.168.1.x to some VPSs and then setup a reverse proxy.

Setup of mod_proxy

Assuming you have debian or ubuntu, its simple:

```
a2enmod proxy
a2enmod proxy_http

/etc/init.d/apache2 restart
```

Config of mod_proxy with a vhost

The following vhost config forwards traffic over port 80 and 443 (https). Of course when a client goes to <https://privatevps.website.com> they will get the ssl cert of the public facing apache server which most likely will be a different domain. In any case they can choose to accept the ssl cert warning.

Features

1. ProxyPreserveHost On means that on apache on the VPS they can setup vhosts as normal and it will work as normal.
2. ServerAlias *domain.net means that any subdomains the client creates, it will just work with the proxy and traffic will be sent to the private VPS.
3. https traffic can be sent. This requires ssl setup on apache first. See [Apache2 SSL PHP5 MySQL5](#)

```
vi /etc/apache2/sites-available/02-proxy-vps1
<VirtualHost *:80>
    ProxyRequests Off
    ProxyPreserveHost On
    ProxyPass / http://192.168.1.3:80/
    ProxyPassReverse / http://192.168.1.3:80/
    ServerName www.domain.net
    ServerAlias *domain.net
    CustomLog /var/log/apache2/access_domain.log combined
    ErrorLog /var/log/apache2/error_domain.log
</VirtualHost>
<VirtualHost *:443>
    ProxyRequests Off
    ProxyPreserveHost On
    ProxyPass / https://192.168.1.3:443/
    ProxyPassReverse / https://192.168.1.3:443/
    ServerName www.domain.net
    ServerAlias *domain.net
    CustomLog /var/log/apache2/access_domain.log combined
    ErrorLog /var/log/apache2/error_domain.log

    SSLProxyEngine On
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
    BrowserMatch "MSIE [2-6]" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
```

Reverse_Proxy_with_apache_mod_proxy

```
# MSIE 7 and newer should be able to use keepalive
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>

a2ensite 02-proxy-vps1
```

Optional Config on Private VPS

One of the main issues with mod_proxy and apache is that in the apache logs on the Private VPS with the private 192.168.1.x IP address, the IP address of the proxy will appear and not (by default) the clients true IP Address. As a result when tailing access.log or error.log on the backend apache server, the ip of the proxy will appear (192.168.1.1). While most people use google analytics or a javascript web traffic method, using webalizer or similar on the backend server won't work.

The Solution

```
apt-get install libapache2-mod-rpaf
a2enmod rpaf

vi /etc/apache2/mods-enabled/rpaf.conf
//Change the following to (where 192.168.1.1 is the proxy IP):
<IfModule mod_rpaf.c>
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 192.168.1.1
</IfModule>

/etc/init.d/apache2 restart
tail /var/log/apache2/access.log
```

Now the true client IP address will show correctly in the access.log behind the proxy server.

Conclusion: this method works very well. I have a single vhost for each Private VPS. By default I add a wildcard domain to send traffic to the private VPS. If the client gets a new domain name, I can add it as a ServerAlias. The ProxyPreserveHost makes this easy.