**Nginx访问控制**

基于IP访问控制 http\_access\_module

基于用户登录认证 http\_auth\_basic\_module

基于IP的访问控制

//允许配置语法

Syntax: allow address | CIDR | unix:| all;

Default: —

Context: http, server, location, limit\_except

//拒绝配置语法

Syntax: deny address | CIDR | unix:| all;

Default: —

Context: http, server, location, limit\_except

//配置拒绝某⼀一个IP, 其他全部允许

location ~ ^/1.html {

root /usr/share/nginx/html;

index index.html;

deny 192.168.56.1;

allow all;

}

//只允许某⼀一个⽹网段访问,其它全部拒绝

location / {

root html;

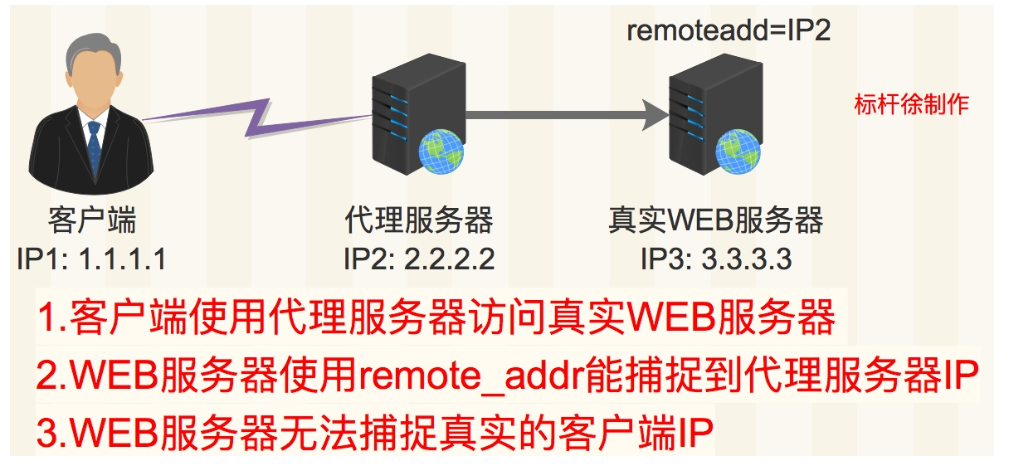
index index.php index.html index.htm;

allow 192.168.56.0/24;

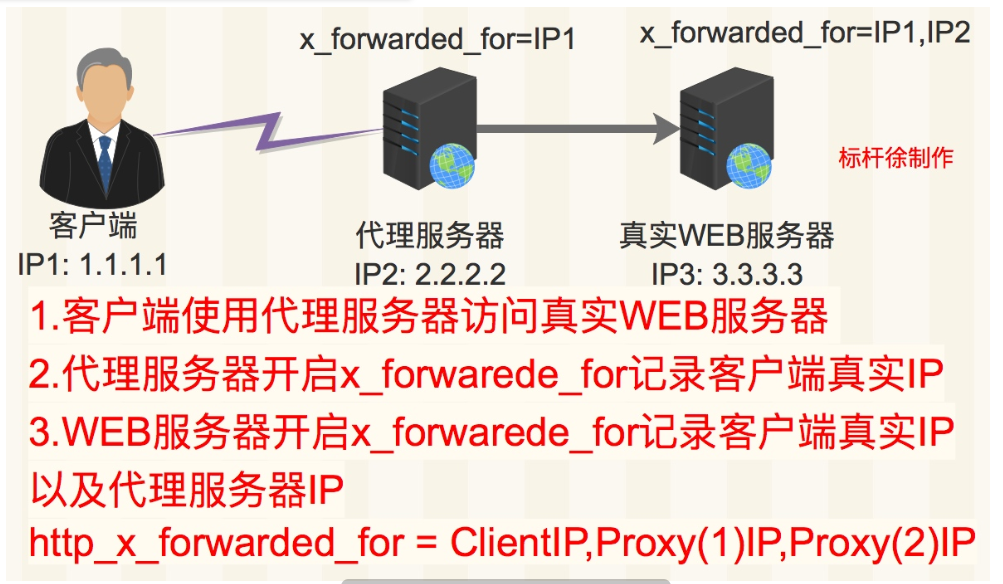
deny all;

}

**http\_access\_module**



下图是使⽤用http\_x\_forwarded\_for记录真实客户端IP地址以及代理理服务器IP



解决⽅方式

1.采⽤用HTTP头信息控制访问, 代理理以及web服务开启http\_x\_forwarded\_for

2.结合geo模块作

3.通过HTTP⾃自动以变量量传递

**基于⽤用户登陆认证**

//配置语法

Syntax: auth\_basic string| off;

Default: auth\_basic off;

Context: http, server, location, limit\_except

//⽤用户密码记录配置⽂文件

Syntax: auth\_basic\_user\_file file;

Default: -

Context: http, server, location, limit\_except

//需要安装依赖组件

[root@xuliangwei ~]# yum install httpd-tools

[root@xuliangwei ~]# htpasswd -c /etc/nginx/auth\_conf xuliangwei

//可在http,server,location下添加如下信息

auth\_basic "Auth access Blog Input your Passwd!";

auth\_basic\_user\_file /etc/nginx/auth\_conf;

**⽤用户认证局限性**

1.⽤用户信息依赖⽂文件⽅方式

2.⽤用户管理理⽂文件过多, ⽆无法联动

3.操作管理理机械，效率低下

**解决办法**

1.Nginx结合LUA实现⾼高效验证

2.Nginx结合LDAP利利⽤用nginx-auth-ldap模块