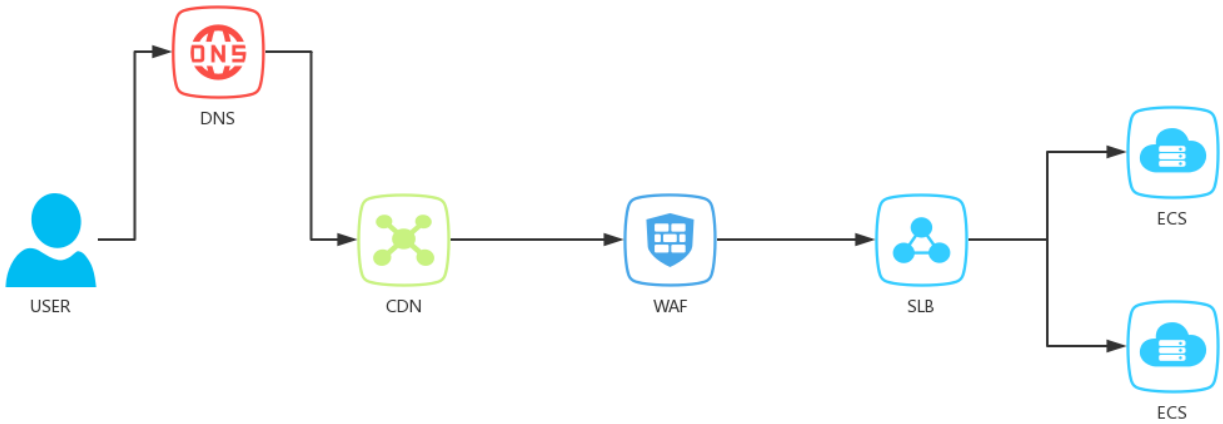
当攻击者发现目标站点存在CDN防护的时候，会尝试通过查找站点的真实IP，从而绕过CDN防护。

我们来看一个比较常见的基于公有云的高可用架构，如下：

CDN（入口层）->WAF（应用层防护）-> SLB（负载层）-> ECS（源站） -> RDS（数据库）

即对应关系为：域名 cname CDN，CDN--->WAF，WAF---> SLB，SLB---> ECS。



我们重点来关注一下CDN--->WAF--->SLB--->ECS这几层服务的关系。

假设，攻击者知道SLB的真实IP地址，就可以直接访问SLB的ip地址，从而轻易绕过CDN+WAF的安全防护。

如何防止CDN被绕过呢？

这里分享一个CDN防护技巧，通过中间件配置只允许域名访问，禁止ip访问。

这样处理的话，所有直接访问站点真实IP的请求都会被拒绝，任何用户只能通过域名访问站点，通过预先设定的网络链路，从DNS-->CDN-->waf防护-->源站，所有的访问请求都必须经过WAF检测。

即使攻击者找到了真实IP地址，修改本地hosts文件，强行将域名与IP解析，也无法访问到目标站点。

Nginx参考配置：

```
#添加一个server,在原server里绑定域名
server  {
        listen 80 default;
        server_name _;
        return 403;
    }
server {
        listen       80;
        server_name  www.demo.com;
        .........
```

Apache参考配置：

```
#在httpd.conf最后面加上

<VirtualHost 此处填写IP>
        ServerName 此处填写IP
        <Location />
            Order Allow,Deny
            Deny from all
        </Location>
</VirtualHost>

<VirtualHost 此处填写IP>
        DocumentRoot /var/www/html
        ServerName   此处填写域名
</VirtualHost>
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。