直播防盗链功能说明

网宿科技股份有限公司

目录

1. 功能概述 - 3 -

2. 功能说明 - 3 -

2.1 基础防盗链 - 4 -

2.1.1 IP 访问控制 - 4 -

2.1.2 Referer 防盗链 - 5 -

2.2 高级防盗链 - 6 -

2.2.1 时间戳防盗链 - 6 -

2.2.2 swf 防盗链 - 9 -

2.2.3 回源鉴权防盗链 - 10 -

1. 功能概述

防盗链的目的是为了确保内容提供商的内容资源在经过CDN分发时不被其他人恶意的引用或者被非法用户下载，从而确保服务的安全性以及避免产生不必要的带宽浪费，为内容提供商节约成本。

根据防盗链规则的复杂程度，网宿的直播防盗链功能可以分为基础防盗链和高级防盗链两大类，可以满足绝大部分客户不同业务不同场景的防盗链需要。

2. 功能说明

本节主要介绍了每一种防盗链的原理、适应场景和注意事项。基础防盗链的规则比较简单，不做过多的说明，重点放在高级防盗链上。

文档中包含的防盗链功能均为通用的，默认可以支持的功能，对于仍然无法满足的防盗链需求，可以单独进行评估开发，但不在本文档的覆盖范围之内。

下面的表格列出了目前主要支持的防盗链种类。

防盗链分类	防盗链验证规则	防盗链名称	应用场景举例
2.1 基础防链	基于访问者 IP	IP 黑白名单	将明确 IP 地址的恶意攻击者，加入黑名单，禁止访问 如企业内部员工使用的系统；或只允许白名单中合法 IP 进行访问
		区域访问限制	禁止或允许某些地区的用户访问某些特定的资源，常用于版权保护
	基于请求 URL	2.1.2 Referer 防盗链	通过 http 请求头中的 Referer 字段来防止网站链接被其他站点非法引用

2.2 高级防链	基于密文、时间串、IP 地址、MD5 算法等	2.2.1 时间戳防盗链	对防盗链可靠性有更高要求的场景下，比如视频独家直播等
	基于 SWF 文件	SWF 防盗链	1、需要客户将 SWF 文件提供给 CDN。 2、仅适用于 RTMP 协议
	基于源的鉴权结果	回源鉴权	1、防盗链实现复杂，需要客户开发鉴权服务器。 2、高度定制化，直播视频产品通常根据自身需要定制不同的防盗链。 3、适用于推拉流端。

上述提及的所有防盗链功能，均支持对需做防盗链判断的请求进行访问控制（允许或禁止）。对于禁止，支持两种类型的拒绝方式：

1. 返回特定的错误状态码来拒绝服务（默认方式，状态码可以指定，默认 403）。
2. 返回 302Found 的重定向 url，重定向的 url 可以指定。

2.1 基础防盗链

基础防盗链主要是针对客户端请求过程中所携带的一些关键信息来验证请求的合法性，比如客户端请求 IP，请求 URL 中携带的 referer。优点是规则简单，配置和使用都很方便，缺点是防盗链所依赖的验证信息很多都是可以伪造的，因此此类防盗链可靠性较低。

2.1.1 IP 访问控制

原理：

IP 地址在互联网上具有唯一性，通常客户端在请求过程中，IP 地址保持不变，客户端向服务端（CDN 节点）发起请求时，服务端可以明确获取到客户端的 IP 地址，因此可以利用 IP 地址的这些特点进行访问控制。

1. 支持 1 个或多个 IP 的访问控制（黑名单或白名单）

2. 支持针对 IP 段进行访问控制（通常采用 IP+子网掩码的表示方式，比如 192.168.1.0/24）
3. 支持区域访问许可。比如，禁止或允许某些地区的用户（根据访问者的 IP 所在的地理位置）访问某些特定的资源，常用于版权保

适用场景举例：

1）发现某些 IP 地址访问次数巨大，属于不正常的访问或者可能是某种攻击行为，这种情况下可以考虑将该 IP 地址加入黑名单，此 IP 地址访问到 CDN 的节点时会被直接拒绝。

2）加速的内容属于公司或者企业的员工内部使用，不希望被企业之外的其他人访问到。企业通常有固定统一的出口 IP 地址，因此可以将这些出口 IP 加入白名单，只允许白名单中的 IP 访问，其他所有 IP 都将被拒绝。

3）有些特殊的资源只希望北京地区的用户使用，禁止其他地区的用户使用，可以使用地区访问许可的功能。

注意事项：暂无

2.1.2 Referer 防盗链

原理：

Referer 在 HTTP 协议里有特殊的用途，当浏览器向服务器发送请求时，一般会带上 Referer 头，告知服务器该请求是从哪个页面链接过来的。Referer 经常被用于页面访问统计、图片防盗链等。

流媒体直播同样支持 Referer 防盗链，当请求发送到 CDN 服务器后，CDN 服务器检查客户 URL 中所携带的 Referer 字段的信息，禁止或者允许符合特定规则（支持正则匹配）的 Referer 的请求。

适用场景举例：

某直播客户，通过 referer 做防盗链。比如 http://cdn.example.com/，访问该页面下的所有直播流时，比如 http://cdn.example.com/live1.flv，浏览器在请求时会自动带上 Referer：http://cdn.example.com/表明请求的来源地址。

注意事项：

1）在使用 Referer 防盗链功能时，应该特别注意指明空引用的处理方式（空引用是指 http 请求头中没有携带 Referer 头部 ,通常是直接在浏览器地址栏访问某个 url 或者通过非浏览器的方式访问某个 url 时，请求头部不会带有 referer 头部；），默认禁止空引用。

2）Referer 很容易伪造，因此 referer 防盗链安全性较低。

2.2 高级防盗链

流媒体直播中，高级防盗链主要是指时间戳防盗链、swf 防盗链、回源鉴权防盗链。

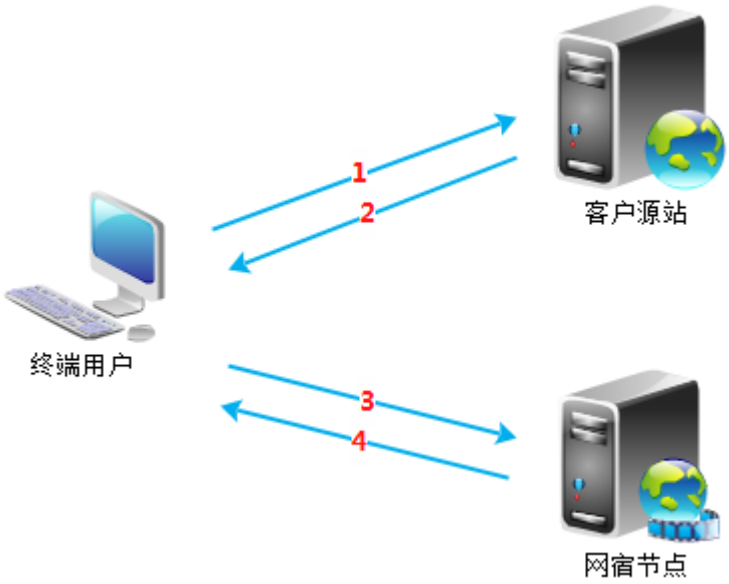
时间戳防盗链的特点是加密的 url 具有时效性，无法伪造，当达到过期时间后 url 不再被允许访问，适合一些对“时效性”有要求的场景，使用时需要内容提供商和 CDN 配合，内容提供商负责生成加密的 url，CDN 负责根据预先设定的规则对 url 进行合法性验证。时间戳防盗链由于实现原理简单、可靠性高，推荐使用。

Swf 防盗链为 RTMP 协议所特有，其特点为需要客户提前将 SWF 文件上传至 CDN 节点，由客户端和 CDN 节点在请求过程中基于一定机理进行加密和解密验证，CDN 验证通过则响应用户请求，验证失败则拒绝用户请求。

回源鉴权的特点是 CDN 节点每次接收到的请求，都需要先回源进行验证，验证通过后才认为请求合法，继续提供服务，适用于对防盗链有很高的实时性要求的场景。另外，一些特殊性的防盗链，CDN 默认不支持的情况下也可以考虑采用回源鉴权的形式。

2.2.1 时间戳防盗链

原理：



1、当用户发起请求时视频请求时，用户的请求会被引导至客户源站。例如，终端用户发起的请求 url 为：http://www.example.com/test.flv

2、客户源站通过一系列参数共同加密生成一串密文。目前网宿可支持客户用于生成密文的参数有客户源站时间、用户请求的直播流、网宿 key（由网宿提供）、IP 地址串。假设客户源站时间为：4d024e80,用户请求的直播流为：test.flv，网宿 key 为：abc，ip 地址为 192.168.1.1，则以上数据经过 md5 加密后，生成的密文为：84579e4b82787870e418004c59f696b0，则客户源站返回给终端用户的 url 为：http://cdn.example.com/test.flv?wsSecret=84579e4b82787870e418004c59f696b0&wsTime=4d024e80

3、终端用户利用客户源站返回的 url，重新向网宿节点发起请求，发起请求的 url 为：http://cdn.example.com/test.flv?wsSecret=84579e4b82787870e418004c59f696b0&wsTime=4d024e80

4、网宿节点进行验证：

a) 根据 url 的加密形式取出对应的过期时间，和当前时间进行比较，确认请求是否过期

b) 根据约定的 md5 计算方式和密文，计算出 md5 加密串后和 url 中原始的加密串进行比较

只有 a）和 b）都验证通过，请求才会被认为是合法的。不合法的请求可以采取禁止访问或者 302 重定向到指定的 url。

使用方法：

1、需要确认的信息

a) 确认过期时间的格式。默认采用的是 Unix 时间戳的形式，比如 1371982466 表示时间是 2013-06-23 18:14:26，支持其他一些时间表达格式，比如：

i. 20130623181426

ii. 2013-06-23

iii. 51c6ca82（推荐此表示方式，将十进制的 1371982466 采用 16 进制表示，，有较好的隐蔽性）

b) 需要确认过期时间。即客户访网宿 URL 中所携带的时间与 CDN 节点当前时间的差值范围。

c) 确认参与 md5 计算的相关参数，以及组合顺序，目前支持的参数包括：

支持的参数	举例
客户端请求的 IP	192.168.1.1
客户源系统时间	时间的形式可以是 年（%Y）月（%m）日（%d）时（%H）分（%M）秒(%S)的自由组合，比如 %Y%m%d%H%M%S（即 20130621129），另外，还支持时间的 unix 时间戳（十进制或十六进制）表示形式，比如 1372390211 或 51cd0343,后者具有更好的隐蔽性

应用场景举例：

1、 适用于对 url 有一定时效性的场景

2、 如果在 md5 加密算法中添加客户端的 ip，可以防止用户观看视频后直接将获取到的视频 URL 粘贴分享出去，提供给他人播放。客户端的 ip 也可以通过 url 中的参数传递。

注意事项：

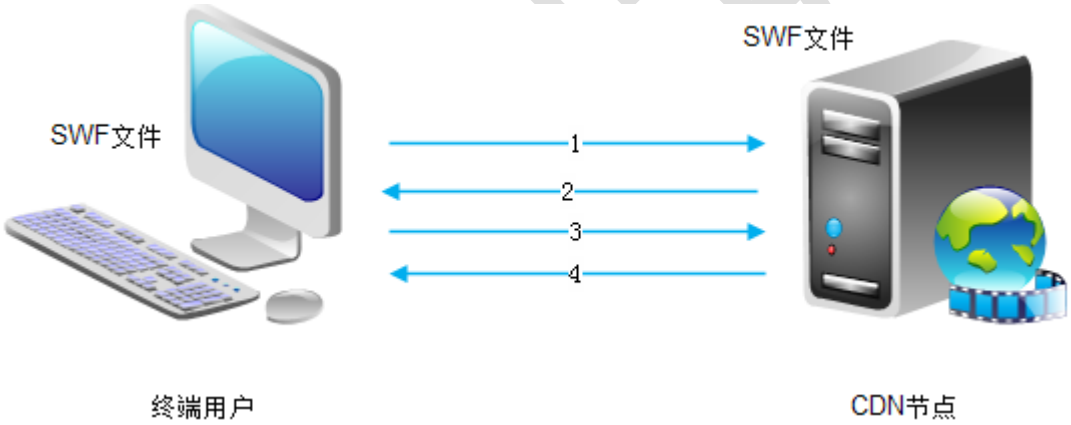
1）时间戳防盗链默认支持，可以直接配置，不需要再次开发

2）当防盗链涉及的参数（比如密文、过期时间等）发生变更时，需要通知 CDN 进行配合更改，原则上密文一旦确定尽量不要发生变动，不然可能导致源和加速节点使用的密文不一致，请求全部验证不通过

3）使用 IP 进行 md5 计算可能带来一些问题：如果加密使用的 IP1，而到 CDN 这边用的是另外一个 IP2，这样就会被禁止访问。

2.2.2swf 防盗链

原理：



用户需要将播放视频对应 flash 播放器的 SWF 文件提前交由 CDN，CDN 会将该文件提前分发至 CDN 节点。用户播放器端，必须为 flash 播放器。

1、终端用户向 CDN 节点请求 RTMP 视频播放。例如：RTMP://www.test.com/live/channel

2、CDN 节点在接收到用户 RTMP 请求时，会对域名进行判断是否需要进行 SWF 防盗验证。若需要进行防盗链验证，则向播放器端发送相应的 SWF 密钥。该密钥由 CDN 节点生成。

3、用户播放器端，将 SWF 文件，及 CDN 发送给播放器的 SWF 密钥，利用加密算法 HMACsha256，生成一个加密值，并回传给 CDN 节点。

4、CDN 节点用客户提交给 CDN 的 SWF 文件，结合发送给终端用户的 SWF 密钥，利用加密算法 HMACsha256，生成一个加密值，与播放器端回传给 CDN 的 KEY 文件进行比对。若比如结果一致，则响应用户播放请求；若比对结果不一致，则拒绝用户播放请求。

应用场景举例：

1、 该验证过程是在 rtmp 协议的握手过程中完成 ,故仅适用于 adobe 播放器的 rtmp 协议。

2、 客户对防盗链需要比较高，又不愿意进行开发时，可直接使用 adobe 播放器所自带的 swf 防盗链。

注意事项：

1、 用户需要提前将 SWF 文件提交到 CDN,并确保提交至 CDN 的 SWF 文件与播放器端的 SWF 文件一致。

2、 确认加密算法。

3、 步骤二中，的 SWF 密钥生成难度需要适配不同的 SWF，属于高度定制化。

2.2.3 回源鉴权防盗链

原理：

1、 终端用户向 CDN 请求视频内容，在请求中携带需要回源鉴权的参数。例如：http://www.test.com/live/channel.flv?key1=vaule1&key2=vaule2 或者 http://www.test.com/live/channel.flv/key1=vaule1/key2=vaule2 ,这两种请求 URL ,CDN 均支持 ,但我们建议用户使用第一种 URL。若使用第二种 URL ,则 CDN 需要先对用户请求 URL 进行改写，并且第二种 URL,需要用户将 key、value 值固定在特定位置上。

2、 CDN 节点可通过 POST 或者 GET 方式向用户鉴权服务器返回需要鉴权的参数，鉴权参数需要用户提前告知 CDN。

3、 鉴权服务器根据 CDN 传送而来的鉴权信息，进行防盗链判断，决定是否允许用户请求该直播视频，并将结果返回给 CDN 节点。

4、 CDN 节点根据客户鉴权服务器返回的结果，响应或者拒绝终端用户的视频请求。

应用场景举例：

1、 客户技术实力比较强，又不希望第三方公司知悉其防盗链原理时，可使用回源鉴权防盗链。

2、 CDN 无法满足客户特殊防盗链需求时，可使用回源鉴权防盗链。

使用方法：

1、告知 CDN，回源鉴权的参数

2、告知 CDN，鉴权服务器地址。

3、告知 CDN，回源鉴权的方式，目前支持 get 及 post 两种

4、告知 CDN，鉴权结果，例如 1 代表成功，0 代表失败

5、告知 CDN，超时等待时间，及超时如何处理，例如，鉴权服务器 3S 不响应，就同意请求，或拒绝请求。

注意事项：

1、每次请求都需要先进行鉴权，在请求量较大时，需要考虑鉴权服务器的压力

2、该鉴权形式客户需要维护专门的鉴权服务器。