

## 域名拦截教程

注：**https** 为加密协议，目前无法拦截。正在努力中，即将实现。

需求背景：

**URL 拦截**：禁止访问新闻、游戏等具体网站，则可根据此教程添加防火墙规则来禁止访问；例如腾讯新闻、东方财富网等。

首先进入“对象管理→URL”，点击“添加”，按下图格式输入想要拦截的域名：

对象管理 / URL / URL对象

URL对象 URL组对象

刷新 + 添

显示数量：20条

ID

1

2

共 2 条记录

新增URL对象

名称 news

组ID 35

URL qq.com  
163.com  
news.cctv.com

备注

确定 取消

\*大小写字母数字和下划线组成

\*组ID值在32-255之间，不能重复

\*有效URL格式：www.xxx.com,xxx.com  
URL之间不能有空格，每行一个，不能超过50000

点击确定后，进入“网络安全→防火墙”，点击“添加”：

新增防火墙

来源地址  新地址项 A.B.C.D/M 或 A.B.C.D-A.B.C.D  来源地址取反

地址对象 WEBCACHE + 添加地址对象分组

目的地址  新地址项 A.B.C.D/M 或 A.B.C.D-A.B.C.D  目的地址取反

地址对象 WEBCACHE + 添加地址对象分组

端口对象  选择服务 any  自定义协议 TCP 端口

时间对象 任意

入接口 LAN0 \*数据包从此接口入

出接口 WAN0 \*数据包从此接口出

更多高级选项  启用

注意选好数据包的入口与出口，一般来说入口为内网口，出口为外网口。也可以在“来源地址”中填写需要禁止访问的主机 IP，则此时入口与出口均为任意。

来源地址   来源地址取反

新地址项 192.168.1.0/24

地址对象 WEBCACHE

目的地址   目的地址取反

新地址项 0.0.0.0/0

地址对象 WEBCACHE

端口对象   端口

选择服务 any

自定义协议 TCP

时间对象 任意

入接口 任意  \*数据包从此接口入

出接口 任意  \*数据包从此接口出

如果只需要在某一时间段内禁止，则按相同的方法在“对象管理尖→时间”中添加时间对象，然后防火墙里选择时间对象。

勾选“更多高级选项”，选择已经建好的 URL 对象，动作选择“拦截”，点击“确定”即可。建议再点击页面右上角的“保存”，以免路由断电后设置丢失。

更多高级选项  启用

状态检测  新建  已建  关联  无效

源MAC地址过滤 eg. 00:0c:29:ba:d0:31  取反  \*MAC地址或MAC地址对象

URL过滤 news  取反

关键字过滤 不启用  取反

数据流方向 不启用

会话匹配 模式: 不启用 方向 请求

范围: 从 0 到 0

并发连接限制 限制并发数 / 有效掩码范围为1-32  \*限制并发数/掩码, 有效掩码范围为1-32

流量限制  启用流量限制

限制速率: / sec  \*eg. 1000(0-10000),100kbit,10mbit

限制模式: / 源IP+目的IP+目的端口  \*地址掩码长度: 1 - 32

限制节点:  \*有效值[1,8388608]

字符串过滤  启用字符串过滤

字符串 匹配位置: 从 到  \*单位: 字节

数据包长度 范围: 从 0 到 0  取反

应用协议 任意

动作 拦截  取反

日志  启用日志  简要记录  详细记录  \*启用日志描述不能为空

日志描述

备注

## 关键字拦截：禁止网页内部分内容显示，如不显示图片等。

进入“对象管理→关键字”，点击“添加”，输入要拦截的域名，点击确定。这里举例拦截腾讯新闻与网易新闻的图片服务器域名，则打开新闻后无法加载图片。

新增关键字对象

名称	<input type="text" value="new"/>	*大小写字母数字和下划线组成
组ID	<input type="text" value="32"/>	*组ID值在32-255之间，不能重复
关键字	<input type="text" value="inews.gtimg.com&lt;br/&gt;pic-bucket.nosdn.127.net"/>	*关键字之间不能有空格，每行一个，不能超过512
备注	<input type="text"/>	

到防火墙中添加，步骤同上，关键字过滤选择刚才建立的对象：

更多高级选项  启用

状态检测  新建  已建  关联  无效

源MAC地址过滤   取反 \*MAC地址或MAC地址对象

URL过滤 不启用  取反

关键字过滤   取反

数据流方向 不启用

会话匹配 模式: 不启用 方向 请求

范围: 从  到

并发连接限制 限制并发数 / 有效掩码范围为1-32 \*限制并发数/掩码，有效掩码范围为1-32

流量限制  启用流量限制

限制速率:  / sec \*eg. 1000(0-10000),100kbit,10mbit

限制模式: / 源IP+目的IP+目的端口 \*地址掩码长度: 1 - 32