HCIE-Security 备考指南

URL 过滤

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security URL 过滤需要掌握的知识点

- 熟悉 WEB 过滤关键技术
- 掌握 WEB 过滤技术的应用

URL 过滤简介

介绍 URL 过滤特性的定义和目的。

定义

URL 过滤功能可以对用户访问的 URL 进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。另外，对于指定 URL 分类的 HTTP 报文，NGFW 可以修改报文中的 DSCP 字段，即 DSCP 优先级，从而便于其他网络设备根据修改后的 DSCP 优先级区分流量，对不同分类的 URL 流量采取差异化处理。

说明：

URL 过滤功能支持过滤 HTTP 协议和 HTTPS 协议的 URL 请求。

目的

随着互联网应用的迅速发展，计算机网络在经济和生活的各个领域迅速普及，使得信息的获取、共享和传播更加方便，但同时也给企业带来了前所未有的威胁：

- 员工在工作时间随意地访问与工作无关的网站，严重影响了工作效率。
- 员工随意访问非法或恶意的网站，造成公司机密信息泄露，甚至会带来病毒、木马和蠕虫等威胁攻击。
- 在内部网络拥堵时段，无法保证员工正常访问与工作相关的网站（如公司主页、搜索引擎等），影响工作效率。

URL 过滤技术可以根据不同的用户/组、时间段和安全区域等信息，对用户/组进行 URL 访问控制，达到精确管理用户上网行为的目的。同时，URL 过滤技术还可以对不同 URL 分类的 HTTP 报文修改其 DSCP 优先级，以便于其他网络设备对不同分类的 URL 流量采取差异化处理。

URL 格式

URL 地址用来完整地描述 Internet 上的网页或者其他资源的地址。

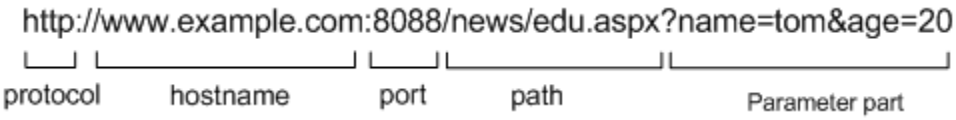
URL 的一般格式为：“protocol://hostname[:port]/path[?query]”。各参数含义如表 1 所示。

表 1 URL 参数解释

字段	含义
protocol	使用的应用协议，最常用的是 HTTP 和 HTTPS 协议。
hostname	Web 服务器的域名或者 IP 地址。
:port	可选，通信端口。各种应用协议都有默认的端口号，如 HTTP 协议的默认端口为 80、HTTPS 协议的默认端口号为 443。当 Web 服务器采用非默认端口时，URL 中不能省略端口号。
path	由零个或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址。
?query	可选，用于给动态网页传递参数。

例如，如图 1 所示，对于“http://www.example.com:8088/news/edu.aspx?name=tom&age=20”：

图 1 URL 格式介绍



- http 为协议。
- www.example.com 为 hostname。
- 8088 为通信端口。
- news/edu.aspx 为 path。
- name=tom&age=20 为参数部分。

URL 匹配方式

URL 匹配方式包括前缀匹配、后缀匹配、关键字匹配、精确匹配。

管理员需要在白名单、黑名单、自定义分类、预定义分类中配置 URL。NGFW 可以通过几种 URL 匹配方式来定义希望匹配的 URL 的范围。

表 1 对几种匹配方式做了简单比较。

表 1 URL 匹配方式

匹配方式	定义	条目	匹配结果
前缀匹配	匹配所有以指定字符串开头的URL。	www.example.com*	匹配所有以 www.example.com 开头的 URL，如： • www.example.com • www.example.com/solutions.do
后缀匹配	匹配所有以指定字符串结尾的URL。	*aspx	匹配所有以 aspx 结尾的 URL，如： • www.example.com/news/solutions.aspx • www.example.com/it/price.aspx • 10.1.1.1/sports/abc.aspx
关键字匹配	匹配所有包含指定字符串的 URL。	*sport*	匹配所有包含 sport 的 URL，如： • sports.example.com/news/solutions.aspx • sports.example.com/it/ • 10.1.1.1/sports/
精确匹配	只匹配指定字符串。	www.example.com/news	只匹配 www.example.com/news 。www.example.com/news/solutions.aspx 、www.example.com/news/en/等不会匹配该条目。

说明：

- 对于所有匹配方式，NGFW 会去除输入字符串中包含的前缀“http://”或“https://”，如果是精确匹配，对于 hostname 字段后没有“/”的字符串会在末尾增加“/”。
- URL 条目不区分大小写。

URL 过滤方式

当用户的 URL 访问请求通过不同的匹配方式匹配到某条 URL 之后，NGFW 会根据配置的 URL 过滤方式对此 URL 访问请求作出相应的处理。

NGFW 提供基于黑白名单和 URL 分类查询的过滤方式，达到精确管理用户上网行为的目的。

- 黑白名单

  NGFW 将解析出的 URL 地址与黑白名单进行匹配，如果匹配白名单则允许该 URL 请求；如果匹配黑名单则阻断该 URL 请求，同时显示 Web 推送页面。

- URL 分类查询

  URL 分类分为自定义分类和预定义分类，一个 URL 分类可以包含若干条 URL，一条 URL 可以属于多个分类。

设备提取 URL 信息后，优先进行自定义分类的查询。如果匹配自定义分类，则按照 URL 过滤配置文件中配置的响应动作进行处理。当控制动作为阻断时，NGFW 将阻断该 URL 请求，同时显示 Web 推送页面。

URL 预定义分类查询分为两种方式：

- 本地缓存查询：设备初次上电时，已经将 URL 预置热点库加载到缓存里。当设备提取了 URL 信息后，首先会在缓存中查询该 URL 对应的分类。如果查询到 URL 分类，则按照 URL 过滤配置文件中配置的响应动作进行处理。当控制动作为阻断时，NGFW 将阻断该 URL 请求，同时显示 Web 推送页面。

  如果查询不到，则到远程分类服务器上继续查询。

- 远程分类服务器查询：该服务器部署在广域网，提供更庞大的 URL 分类信息。当本地缓存中查询不到 URL 对应的分类时，设备将该 URL 送入远程查询服务器继续查询。如果查询到 URL 对应的分类，则按照 URL 过滤配置文件中配置的响应动作进行处理，并将该 URL 和其对应的分类信息保存到本地缓存中，以便下次快速查询。当控制动作为阻断时，NGFW 将阻断该 URL 请求，同时显示 Web 推送页面。

  如果查询不到，则按照分类为“其他”的响应动作进行处理。

  说明：

  远程分类服务器查询需要购买 License 后才能使用。

  设备运行一段时间后，缓存的内容会不断更新，并以文件的形式保存到存储介质中。当设备重启后，系统会自动加载保存的缓存信息，减少远程分类服务器查询的过程。

URL 过滤的控制动作包括允许、告警和阻断，其严格程度依次增高。对属于多个分类的 URL 的响应动作将按照最严格的动作执行。

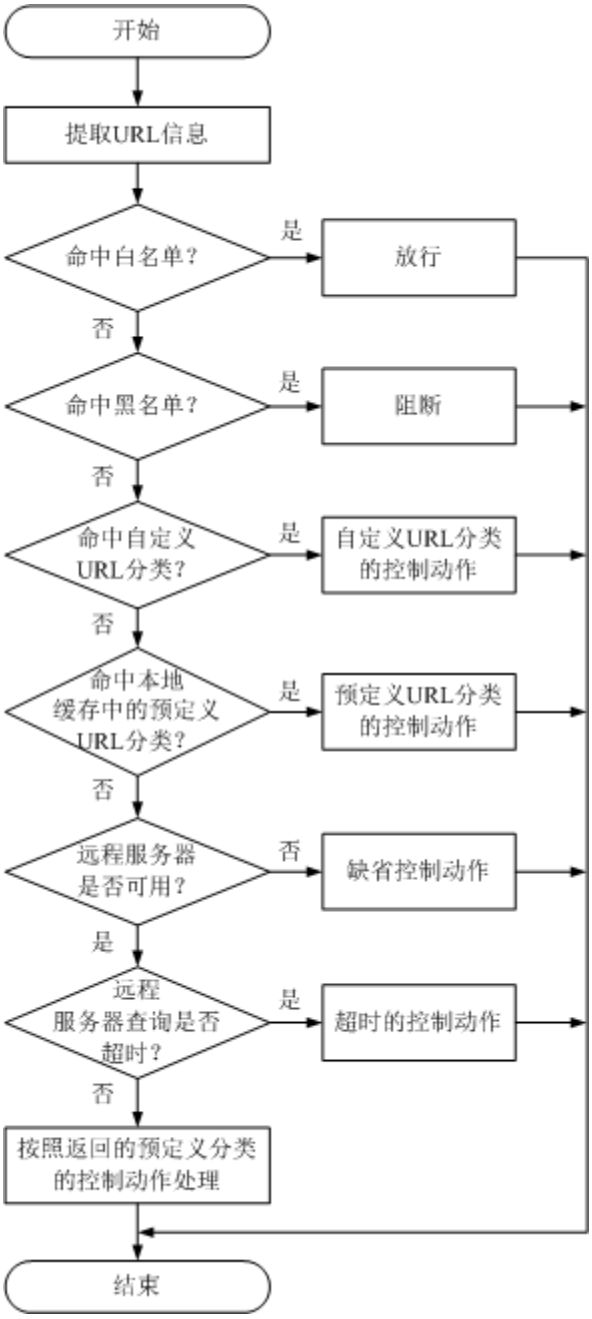
- 允许：指允许用户访问请求的 URL。
- 告警：指允许用户访问请求的 URL，同时记录日志。
- 阻断：指阻断用户访问请求的 URL，同时记录日志。

URL 过滤处理流程

介绍 NGFW 进行 URL 过滤的处理流程。

在 NGFW 启用 URL 过滤功能的情况下，当用户通过 NGFW 使用 HTTP 或 HTTPS 访问某个网络资源时，NGFW 将进行 URL 过滤。处理流程如图 1 所示：

图 1 URL 过滤处理流程图



1. 用户发起 URL 访问请求，如果数据流匹配了安全策略，且安全策略的动作为允许，则进行 URL 过滤处理流程。
2. NGFW 将 URL 信息与白名单进行匹配。
   - 如果匹配白名单，则允许该请求通过。
   - 如果未匹配白名单，则进行下一步检测。

3. NGFW 将 URL 信息与黑名单进行匹配。
   - 如果匹配黑名单，则阻断该请求。
   - 如果未匹配黑名单，则进行下一步检测。
4. NGFW 将 URL 信息与自定义分类进行匹配。
   - 如果匹配自定义分类，则按照自定义 URL 分类的控制动作处理请求。

     说明：

     管理员自行向预定义分类中添加的 URL 属于自定义分类的 URL。
   - 如果未匹配自定义分类，则进行下一步检测。
5. NGFW 将 URL 信息与本地缓存中的预定义分类进行匹配。
   - 如果在本地缓存中查询到对应的分类，则按照该分类的控制动作处理请求。
   - 如果在本地缓存中没有查询到对应的分类，则进行远程服务器分类查询。
     - 如果远程服务器可用，则继续进行远程服务器分类查询。
     - 如果远程服务器不可用，则按照缺省动作处理请求。
6. 启动远程服务器分类查询。
   a. 如果远程服务器分类查询超时，则按照管理员配置的预定义分类查询超时的动作处理。
   b. 如果 URL 分类服务器明确查询到该 URL 属于预定义分类的某个分类，则按照该分类的控制动作处理。

使用限制和注意事项

配置 URL 过滤前请先阅读使用限制和注意事项。

- URL 过滤功能只支持过滤 HTTP 协议和 HTTPS 协议的 URL 请求。
- URL 分类远程服务器查询功能受 License 控制。当 License 过期后，URL 分类远程服务器查询功能不可用。
- URL 分类远程服务器查询功能需要配置服务器所在国家，否则 URL 分类远程服务器查询功能不可用。

URL 过滤应用场景

URL 过滤功能通常用于企业网关，精确管理用户使用 HTTP 或 HTTPS 访问网络资源的行为。

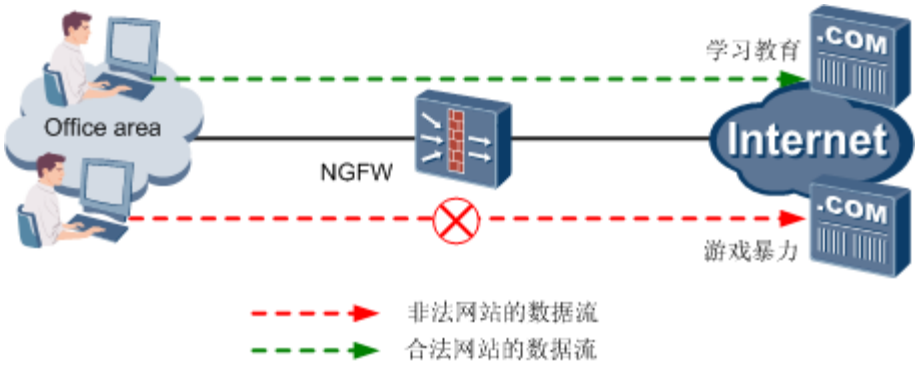
NGFW 作为企业网关部署在网络边界，当企业用户发起 HTTP 或 HTTPS 的 URL 请求时，通过 URL 过滤功能可以实现对用户的请求进行放行、告警或者阻断。

如图 1 所示，使用 URL 过滤后：

- 当用户访问合法的网站时，放行此请求，并选择是否重标记报文的 DSCP 优先级。
- 当用户访问非法的网站时，阻断此请求。

URL 过滤还可以通过引用时间段或用户/组等配置项，实现针对不同时间段或不同用户/组的请求进行放行或者阻断，达到更加精细化和准确化控制员工上网权限的需求。

图 1 URL 过滤的典型应用场景



配置 URL 分类

URL 分类分为自定义分类和预定义分类，管理员可以利用系统提供的预定义分类，也可以创建自定义分类，达到对 URL 进行过滤的目的。

背景信息

预定义分类和自定义分类的使用场景分别如下，请根据需求选择配置：

- 预定义分类：

  预定义分类已经预先对大量常见的 URL 进行了分类，管理员可以根据这些分类轻松地控制内网用户禁止访问哪些类别的 URL、允许访问哪些类别的 URL。

预定义分类是系统内置的，管理员不能够创建、删除和重命名预定义分类，但可以向预定义分类中添加自定义的 URL 规则。

- 自定义分类：

虽然预定义分类库覆盖了主流的 Web 网站，但很多新出现的网站可能覆盖不到。另一方面，管理员出于特殊的过滤需求或者增强预定义预置库等目的，也会按需创建一些对应的自定义分类，定制一批网站的安全策略。此时可以通过配置自定义分类来满足需求。

配置自定义分类

1. 选择“对象 > URL 分类”。
2. 配置自定义分类时，可以单击“新建”，创建自定义分类；也可以单击“导入”，批量创建自定义分类。
   - 创建自定义分类。
     a. 单击“新建”。
     b. 配置 URL 自定义分类。

参数	说明
名称	输入 URL 自定义分类的名称。
描述	输入 URL 自定义分类的描述信息。
URL	输入需要自定义的 URL。 系统预处理后的长度范围是 4～80 个字符。 输入的 URL 中，至少包含 4 个连续的有效字符。通配符“*”不属于有效字符。 通配符“*”，可以出现在 URL 的开始或结束位置。 系统预处理是指去除输入的字符串中包含的前缀“http://”或“https://”，如果是精确匹配，对于 hostname 字段后没有“/”的字符串会在末尾增加“/”。

     c. 单击“确定”。
   - 批量创建自定义分类。
     a. 单击“导入”，在“导入”中单击“CSV 模板”，下载 CSV 模板并保存到本地。按照如图 1 所示的格式填写 CSV 模板。

图 1 CSV 文件格式示意图

类型	名称	ID	描述	URL
1	aaa	100	Profile for marketing	www.example.com
1	bbb	101	Profile for research	www.example.org

b. 配置导入的参数。

参数	说明
从文件中导入 URL	单击“浏览”，选择已经编辑好的 CSV 文件，单击“打开”，完成 CSV 文件的选择。
当前自定义 URL 存在时，覆盖本地自定义 URL 记录	当自定义 URL 分类已经存在时： ▪ 如果选中复选框，导入时 NGFW 会覆盖已存在的 URL 分类。 ▪ 如果不选中复选框，导入时 NGFW 会将此 URL 分类中的 URL 叠加。

c. 单击“开始导入”。

导入完成后，在“用户自定义”下可以看到导入的所有自定义分类。

3. 单击界面右上角的“提交”。

URL 分类变更后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对 URL 分类的操作后再统一进行提交。

添加 URL 到预定义分类中

1. **可选：**如果系统检测到您尚未加载 URL 预定义分类库，请单击“立即加载”。

a. 单击“浏览”，选择待加载的 URL 预定义分类库文件，单击“打开”。

说明：

如果本地没有 URL 预定义分类库文件，请登录安全服务中心 sec.huawei.com，在“特征库下载”处选择对应的产品型号和版本号，下载 URL 热点库文件的最新版本，具体下载方法请参见安全服务中心的帮助信息。

如果设备 CF 卡损坏，则 URL 预定义分类库无法成功加载，请联系技术支持工程师。

b. 单击“开始加载”，操作完成后，可以看到加载成功的 URL 预定义分类。

2. 选择“对象 > URL 分类”。

3. 在“URL 分类”中，单击需要添加 URL 的预定义分类右侧的或选中某个分类后单击分类名称。

4. 添加 URL 到预定义分类中。

参数	说明
名称	URL 预定义分类的名称，无需手工输入。
描述	URL 预定义分类的描述信息，无需手工输入。
URL	输入需要添加的 URL。 系统预处理后的长度范围是 4～80 个字符。 输入的 URL 中，至少包含 4 个连续的有效字符。通配符“*”不属于有效字符。 通配符“*”，可以出现在 URL 的开始或结束位置。 预处理是指去除输入的字符串中包含的前缀“http://”或“https://”，如果是精确匹配，对于 hostname 字段后没有“/”的字符串会在末尾增加“/”。

5. 单击“确定”。
6. 单击界面右上角的“提交”。

URL 分类变更后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对 URL 分类的操作后再统一进行提交。

后续处理

导出 URL 自定义分类是指将 URL 自定义分类以 CSV 文件的格式导出到 NGFW 之外的存储介质上。管理员可以将 URL 自定义分类导出到 CSV 文件中作为备份，后续也可以将导出的 CSV 文件再导入到设备中，实现批量创建 URL 自定义分类的需求。

1. 选择“对象 > URL 分类”。
2. 单击“导出”。
3. 将 URL 自定义分类以 CSV 文件的格式保存到 NGFW 之外的存储介质（如管理员的 PC）上。

配置 URL 过滤

URL 过滤配置文件通过配置黑白名单、自定义分类和预定义分类的控制动作，确定对 URL 进行放行或阻断。使用预定义分类的远程查询功能时，需要配置 URL 分类服务器。

前提条件

如果使用预定义分类，需要首先完成以下方面：

- 请确保 License 已经激活并且在有效服务期。
- 在配置远程服务器查询前，请确保设备与安全服务中心路由可达。

背景信息

白名单的优先级高于黑名单的优先级，两者的使用场景分别如下，请根据需求选择配置：

- 黑名单：

  为了提高员工上班时间的工作效率，优化公司的网络带宽，需要对员工的上网行为进行控制，不允许访问一些娱乐、游戏、视频等网站。

  通过配置 URL 黑名单，阻止用户访问黑名单中定义的 URL 网站。

- 白名单：

  企业有一些特殊需求，对某些网站或某类网站豁免，不需要过滤。

  通过配置 URL 白名单，允许用户访问白名单中定义的 URL 网站。

NGFW 中存在一个 URL 过滤的缺省配置文件，名称为 default。缺省配置文件定义了配置文件的缺省动作为允许，恶意网站的响应动作阻断，其他分类的响应动作均为允许。缺省配置文件不能被修改和删除。

NGFW 支持创建自定义配置文件，您可以根据需要，对每种分类应用不同的响应动作。

操作步骤

1. 选择“对象 > 安全配置文件 > URL 过滤”。
2. **可选：**如果启用了 URL 预定义分类功能，请配置 URL 分类服务器。
   a. 单击“配置”，完成以下参数的配置。

参数	说明
国家	选择设备所在的国家/地区。不配置国家信息或配置不属于设备所在地的国家信息时，禁用 URL 预定义分类查询功能。 **注意：** 请仔细阅读弹出的声明，并在所适用法律法规允许的目的和范围内启用 URL 过滤预定义分类远程查询功能。
安全服务中心	默认为 sec.huawei.com，无需手工输入。

参数	说明
超时时间	输入服务器查询的超时时间。
超时后动作	选择分类服务器查询超时后的处理工作，分为以下几种： • 允许：放行该 URL。 • 告警：放行该 URL，同时记录日志。 • 阻断：阻断该 URL，同时记录日志。 缺省情况下，查询预定义分类超时动作为允许。

b. 单击“确定”。

c. 在弹出的“免责声明”中单击“接受”。

d. 选择“网络 > DNS > DNS”。

e. 在“服务器列表”中输入由运营商提供的 DNS 服务器的 IP 地址。

f. 单击“添加”。

说明：

配置 URL 分类服务器完成后，请检查“URL 分类服务器的连接状态”（“对象 > 安全配置文件 > URL 过滤”）：

- 连接中：表示正在建立连接。请观察 90s，看连接状态是变成了“已连接”还是“未连接”，然后根据以下相应的状态进行处理。
- 已连接：表示已经建立连接。系统会定时地与安全服务中心通信，获取最新的预定义分类。
- 未连接：表示没有建立连接。请检查 DNS 的配置（配置路径：“网络 > DNS > DNS”）、物理连接和路由，确保连接到安全服务中心。

3. 在“URL 过滤配置文件”中，单击“新建”。

4. 配置 URL 过滤配置文件。

参数	说明
名称	输入 URL 过滤配置文件的名称。
描述	输入 URL 过滤配置文件的描述信息。 合理填写描述信息有助于管理员正确理解 URL 过滤配置文件的功能，使 URL 过滤配置文件方便选择、查找和维护。
缺省动作	选择 URL 过滤配置文件的缺省动作，包括允许、告警和阻断三种。 • 允许：放行该 URL。 • 告警：放行该 URL，同时记录日志。 • 阻断：阻断该 URL，同时记录日志。
白名单	输入需要加入白名单的 URL。

<table>
<tr><th colspan="2">参数</th><th>说明</th></tr>
<tr><td colspan="2">黑名单</td><td>输入需要加入黑名单的 URL。</td></tr>
<tr><td rowspan="3">URL 过滤级别
说明：
URL 过滤级别仅针对预定义分类，与自定义分类无关，即选择 URL 过滤级别不会改变自定义分类的处理动作，设置自定义分类的处理动作不会改变 URL 过滤级别。
自定义分类的处理动作需要管理员逐一手工设置，默认为允许。</td><td>高</td><td rowspan="2">选择“高”、“中”或“低”后，系统会对每个预定义分类都设置一个初始的处理动作，对于响应动作为“允许”的 URL 分类，您还可以选择是否配置“重标记报文优先级”。
“高”代表相对比较严格的处理动作，“低”代表相对比较宽松的分类处理动作。</td></tr>
<tr><td>中</td></tr>
<tr><td>低</td><td rowspan="2">选择“自定义”后，所有预定义分类的处理动作设置为“允许”，您还可以选择是否配置“重标记报文优先级”。
说明：
• 当之前已经选择了“高”、“中”或“低”，那么再选择“自定义”后，预定义分类的动作将保持原有 URL 过滤级别对应的设置。
• 选择“高”、“中”或“低”后，手动调整某个预定义分类的动作，这时“URL 过滤级别”将会变成“自定义”。</td></tr>
<tr><td>自定义</td></tr>
</table>

5. 单击“确定”。
6. 在安全策略上引用配置文件。
7. 单击“提交”。

创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。
2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

举例：配置 URL 过滤

在 NGFW 上配置 URL 过滤功能，对用户访问的 URL 进行控制，允许或禁止用户访问某些网页资源。

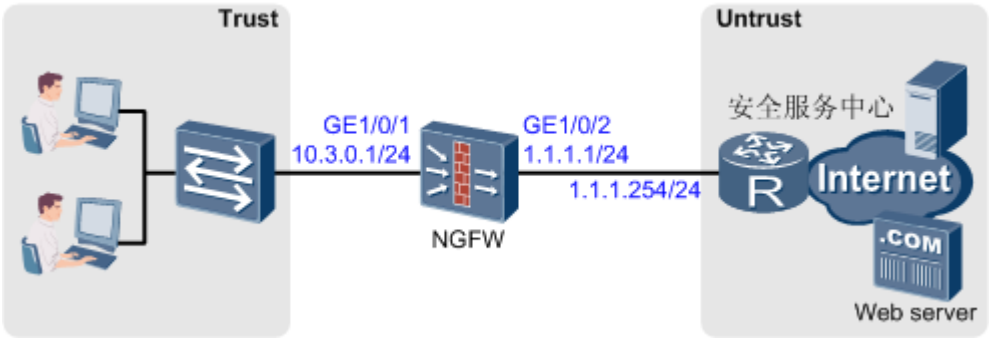
组网需求

如图 1 所示，NGFW 作为企业网关部署在网络边界，对用户发出访问外部网络的 HTTP 和 HTTPS 请求进行 URL 过滤。

公司有研发部门员工和市场部门员工两类，具体需求如下：

- 企业所有员工可以访问包含 education 的网站。
- 企业所有员工不可以访问包含 bbs 的网站。
- 研发部门员工在每天的 09：00～17：00 只可以访问教育/科学类、搜索/门户类网站。其他网站都不能访问。
- 市场部门员工在每天的 09：00～17：00 只可以访问教育/科学类、搜索/门户类、社会焦点类网站和 www.example.com。其他网站都不能访问。

图 1 配置 URL 过滤组网图



配置思路

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
2. 配置自定义分类 url_userdefine_category，将 www.example.com 列入 url_userdefine_category 分类。
3. 配置分类服务器远程查询，用来获取 URL 与预定义分类的对应关系。本例中教育/科学类、搜索/门户类、社会焦点类网站可以通过预定义分类来进行 URL 过滤控制。
4. 针对研发部门员工和市场部门员工，配置两个 URL 过滤配置文件，将包含关键字 bbs 的 URL 列入黑名单，将包含关键字 education 的 URL 列入白名单。并设置 URL 自定义分类和预定义分类的控制动作。
5. 配置两个安全策略，引用时间段、用户组等信息，实现针对不同用户组和不同时间段的 URL 访问控制策略。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。

   a. 选择“网络 > 接口”。

   b. 单击 GE1/0/1 对应的，按如下参数配置。

安全区域	trust
IPv4	
IP 地址	10.3.0.1/24

   c. 单击“完成”。

   d. 参考上述步骤按如下参数配置 GE1/0/2 接口。

安全区域	untrust
IPv4	
IP 地址	1.1.1.1/24

2. 配置 URL 自定义分类。

   a. 选择“对象 > URL 分类”。

   b. 单击“新建”，按如下参数配置。

名称	url_userdefine_category
描述	url userdefine category of access control for marketing.
URL	www.example.com

   c. 单击“确定”。

3. 配置 URL 分类服务器。

   a. 选择“对象 > 安全配置文件 > URL 过滤”。

   b. 单击“配置”，配置 URL 分类服务器，按如下参数配置。

国家	中国
安全服务中心	sec.huawei.com
超时时间	3
超时后动作	允许

   c. 单击“确定”。

d. 单击“接受”。

4. 配置 URL 过滤配置文件。

a. 选择“对象 > 安全配置文件 > URL 过滤”。

b. 在“URL 过滤配置文件”中，单击“新建”，按如下参数配置。

名称	profile_url_1
描述	URL filter profile of web access control for research.
缺省动作	允许
白名单	*education*
黑名单	*bbs*
URL 过滤级别	选择“自定义”：将预定义分类“教育/科学类”和“搜索/门户类”的动作配置为允许，其他预定义分类的动作配置为阻断。 **窍门：** 为了使配置简单化，配置上述动作时，可以采取如下操作： 选择“自定义”后，选中第一行“名称”右侧对应的动作“阻断”，此时所有自定义和预定义分类的动作都成为“阻断”，然后再配置上述两个预定义分类的动作为“允许”。

c. 单击“确定”。

d. 在“URL 过滤配置文件”中，单击“新建”，按如下参数配置。

名称	profile_url_2
描述	URL filter profile of web access control for marketing.
缺省动作	允许
白名单	*education*
黑名单	*bbs*
URL 过滤级别	选择“自定义”：将预定义分类“教育/科学类”、“搜索/门户类”和“社会焦点类”以及自定义分类“url_userdefine_category”的动作配置为允许，其他预定义分类的动作配置为阻断。 **窍门：** 为了使配置简单化，配置上述动作时，可以采取如下操作： 选择“自定义”后，选中第一行“名称”右侧对应的动作“阻断”，此时所有自定义和预定义分类的动作都成为“阻断”，然后再配置上述三个预定义分类及一个自定义分类的动作为“允许”。

e. 单击“确定”。

5. 配置时间段。

a. 选择“对象 > 时间段”。

b. 单击“新建”，按如下参数配置名为“time_range”的时间段。

名称	time_range
类型	周期时间段
开始时间	09：00
结束时间	17：00
每周生效时间	星期一、星期二、星期三、星期四、星期五、星期六、星期日

c. 单击“确定”。

6. 在安全策略中应用 URL 过滤配置文件。

说明：

本例中引用到的用户组 research（研发部门员工）和用户组 marketing（市场部门员工）假设已经创建完成。

a. 选择“策略 > 安全策略 > 安全策略”。

b. 单击“新建”，按如下参数配置。

名称	policy_sec_1
描述	Security policy of web access protect for research.
源安全区域	trust
目的安全区域	untrust
用户	/default/research
时间段	time_range
动作	permit
内容安全	
URL 过滤	profile_url_1

c. 单击“确定”。

d. 单击“新建”，按如下参数配置。关于安全策略的更多信息，请参见安全策略。

名称	policy_sec_2
描述	Security policy of web access protect for marketing.
源安全区域	trust

目的安全区域	untrust
用户	/default/marketing
时间段	time_range
动作	permit
内容安全	
URL 过滤	profile_url_2

e. 单击“确定”。

7. 单击界面右上角的“保存”，在弹出的对话框中单击“确定”。

8. 单击界面右上角的“提交”，在弹出的对话框中单击“确定”。

结果验证

- 企业任何员工都可以访问包含关键字 education 的网站。管理员通过查看 URL 日志（“监控 > 日志 > URL 日志”），可以看到访问包含 education 的 URL 时，命中了过滤类型为“白名单”的 URL 日志信息。
- 企业任何员工访问包含关键字 bbs 的网站时，都被阻断不能访问。管理员通过查看 URL 日志（“监控 > 日志 > URL 日志”），可以看到访问包含 bbs 的 URL 时，命中了过滤类型为“黑名单”的 URL 日志信息。
- 研发部门任何员工在 09：00～17：00 之间，可以访问教育/科学类、搜索/门户类网站，但是访问社会焦点类、论坛类等网站时，都被阻断不能访问。管理员通过查看 URL 日志（“监控 > 日志 > URL 日志”），可以看到研发部门员工访问社会焦点类、论坛类等网站时，命中了过滤类型为“预定义”以及动作为“阻断”的日志信息。
- 市场部门任何员工在 09：00～17：00 之间，可以访问教育/科学类、搜索/门户类、社会焦点类网站和 www.example.com，但是访问论坛类等网站时，都被阻断不能访问。管理员通过查看 URL 日志（“监控 > 日志 > URL 日志”），可以看到市场部门员工访问论坛类等网站时，命中了过滤类型为“预定义”以及动作为“阻断”的日志信息。

配置了 URL 过滤没有生效

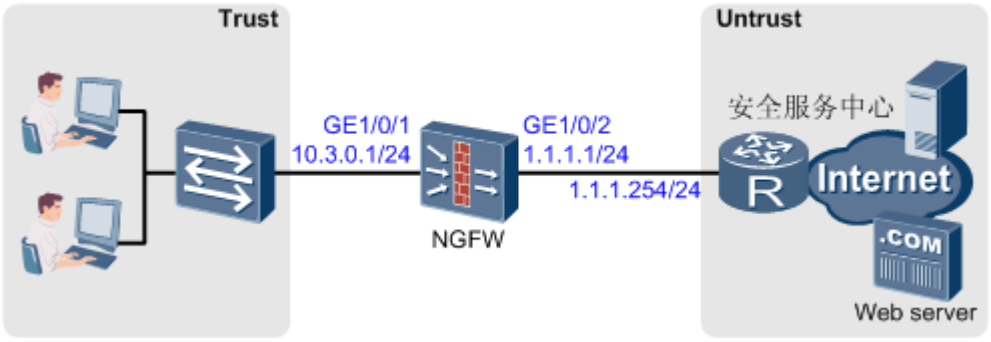
配置了某 URL 的控制动作为阻断，但用户仍然可以访问。

现象描述

管理员已经将某 URL 加入预定义分类，并且配置的控制动作为阻断，但用户仍然可以访问此 URL。

典型组网如图 1 所示。

图 1 URL 过滤组网图



处理步骤

选择“监控 > 日志 > URL 日志”，查看到此 URL 被阻断的日志信息。

可能原因及相应的处理步骤如下：

1. 此 URL 同时加入了白名单。

   说明：

   由于白名单的优先级高于预定义分类的优先级，如果此 URL 同时加入了白名单，那么用户仍然可以访问。

   选择“对象 > 安全配置文件 > URL 过滤”，在“URL 过滤配置文件”中，查看已有配置文件的白名单中是否包含了此 URL。

   - 如果已有配置文件的白名单中包含了此 URL，请将此 URL 从白名单中删除。
   - 如果已有配置文件的白名单中没有包含此 URL，请进行其他项目检查。

2. 用户/组没有在安全策略中应用或者应用错误。

   选择“策略 > 安全策略 > 安全策略”，单击源安全区域（trust）到目的安全区域（untrust）对应的安全策略，查看“用户”配置是否正确。

   - 如果安全策略中“用户”没有配置或者配置错误，请单击“用户”后的下拉列表，选择对应的用户，并单击“确定”，将正确的用户/组应用到安全策略中。
   - 如果安全策略中已经应用了正确的用户/组，请进行其他项目检查。

选择“监控 > 日志 > URL 日志”，没有查看到此 URL 被阻断的日志信息。

可能原因及相应的处理步骤如下：

3. 流量匹配了优先级更高的安全策略规则。

   选择“策略 > 安全策略 > 安全策略”，查看流量是否匹配了其他优先级更高的安全策略。

   - 如果是，则在那条安全策略上应用 URL 过滤配置文件或调整安全策略的顺序。
   - 如果不是，请进行其他项目检查。

4. URL 过滤配置文件没有在安全策略中应用。

   选择“策略 > 安全策略 > 安全策略”，单击源、目的安全区域对应的安全策略，在“内容安全”区域框中，查看“URL 过滤”中是否引用了 URL 过滤配置文件。

   - 如果安全策略中没有引用 URL 过滤配置文件，请单击“URL 过滤”后的下拉列表，选择对应的 URL 过滤配置文件，并单击“确定”，将 URL 过滤配置文件应用到安全策略中。
   - 如果安全策略中已经引用 URL 过滤配置文件，请进行其他项目检查。

5. 修改后的 URL 过滤配置文件未提交编译。

   如果 URL 过滤配置文件有修改但未提交，请单击右上角的“提交”按钮进行编译。

   说明：

   提交黑白名单或自定义、预定义 URL 分类配置会导致配置信息重新编译，对性能有一定影响。如果后续还有黑白名单或者自定义、预定义分类的配置修改，建议完成所有配置修改后提交。

配置了 URL 过滤后阻断了正常网站的访问

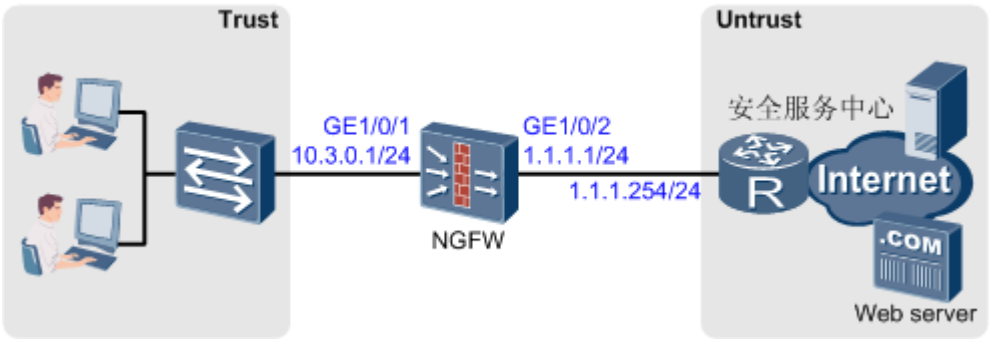
配置了 URL 过滤后，导致某正常的 URL 访问被阻断。

现象描述

管理员已经将某个 URL 加入了预定义分类，并且配置的控制动作为允许，但用户访问此 URL 时失败。

典型组网如图 1 所示。

图 1 URL 过滤组网图



处理步骤

选择“监控 > 日志 > URL 日志”，查看到此 URL 被阻断的日志信息。

可能原因及相应的处理步骤如下：

1. 此 URL 同时加入了黑名单。

   说明：

   由于黑名单的优先级高于预定义分类的优先级，如果此 URL 同时加入了黑名单，那么用户访问此 URL 失败。

   选择“对象 > 安全配置文件 > URL 过滤”，在“URL 过滤配置文件”中，查看已有配置文件的黑名单中是否包含了此 URL。

   - 如果已有配置文件的黑名单中包含了此 URL，请将此 URL 从黑名单中删除。
   - 如果已有配置文件的黑名单中没有包含此 URL，请进行其他项目检查。

2. 此 URL 同时加入了自定义分类，并且配置的控制动作为阻断。

   说明：

   如果此 URL 即加入了自定义分类，又加入了预定义分类，NGFW 会按照两个分类中配置的比较严格的动作**阻断**处理，因此用户访问此 URL 失败。

   选择“对象 > 安全配置文件 > URL 过滤”，在“URL 过滤配置文件”中，查看已有配置文件的自定义分类中是否包含了此 URL。

   - 如果已有配置文件的自定义分类中包含了此 URL，请将此 URL 从自定义分类中删除。

- 如果已有配置文件的自定义分类中没有包含此 URL，请进行其他项目检查。

3. 用户/组没有在安全策略中应用或者应用错误。

   选择“策略 > 安全策略 > 安全策略”，单击源安全区域（trust）到目的安全区域（untrust）对应的安全策略，查看“用户”配置是否正确。

   - 如果安全策略中“用户”没有配置或者配置错误，请单击“用户”后的下拉列表，选择对应的用户，并单击“确定”，将正确的用户/组应用到安全策略中。
   - 如果安全策略中已经应用了正确的用户/组，请进行其他项目检查。

选择“监控 > 日志 > URL 日志”，没有查看到此 URL 被阻断的日志信息。

可能原因及相应的处理步骤如下：

4. 流量匹配了优先级更高的安全策略规则。

   选择“策略 > 安全策略 > 安全策略”，查看流量是否匹配了其他优先级更高的安全策略。

   - 如果是，则在那条安全策略上应用 URL 过滤配置文件或调整安全策略的顺序。
   - 如果不是，请进行其他项目检查。

5. URL 过滤配置文件没有在安全策略中应用。

   选择“策略 > 安全策略 > 安全策略”，单击源、目的安全区域对应的安全策略，在“内容安全”区域框中，查看“URL 过滤”中是否引用了 URL 过滤配置文件。

   - 如果安全策略中没有引用 URL 过滤配置文件，请单击“URL 过滤”后的下拉列表，选择对应的 URL 过滤配置文件，并单击“确定”，将 URL 过滤配置文件应用到安全策略中。
   - 如果安全策略中已经引用 URL 过滤配置文件，请进行其他项目检查。

6. 修改后的 URL 过滤配置文件未提交编译。

   如果 URL 过滤配置文件有修改但未提交，请单击右上角的“提交”按钮进行编译。

   说明：

   提交黑白名单或自定义、预定义 URL 分类配置会导致配置信息重新编译，对性能有一定影响。如果

后续还有黑白名单或者自定义、预定义分类的配置修改，建议完成所有配置修改后提交。

HCIE-Security 模拟面试问题及面试建议

1. URL 过滤处理流程是什么？