目 录

1 URL过滤

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

系列	型号	特性	描述
WX2500H-WiNet系列	WX2510H-PWR-WiNet WX2560H-WiNet	URL过滤	不支持
WX3500H-WiNet系列	WX3508H-WiNet		支持

1.1 URL过滤简介

URL 过滤功能是指对用户访问的 URL 进行控制，即允许或禁止用户访问的 Web 资源，达到规范用户上网行为的目的。

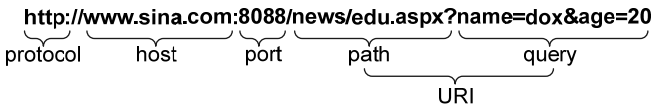
目前，仅支持对基于 HTTP 协议的 URL 进行过滤。

1.1.1 URL过滤原理

1. URL简介

URL（Uniform Resource Locator，统一资源定位符）是互联网上标准资源的地址。URL用来完整、精确的描述互联网上的网页或者其他共享资源的地址，URL格式为：“protocol://host[:port]/path/[;parameters][?query]#fragment”，格式示意如 图 1-1 所示：

图1-1 URL 格式示意图



URL各字段含义如 表 1-1 所示：

表1-1 URL 各字段含义表

字段	描述
protocol	表示使用的传输协议，例如HTTP
host	表示存放资源的服务器的主机名或IP地址
[:port]	（可选）传输协议的端口号，各种传输协议都有默认的端口号
/path/	是路径，由零或多个“/”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
[parameters]	（可选）用于指定特殊参数
[?query]	（可选）表示查询用于给动态网页传递参数，可有多个参数，用“&”符号隔开，每个参数的名和值用“=”符号隔开

字段	描述
URI	URI（Uniform Resource Identifier，统一资源标识符）是一个用于标示某一互联网资源名称的字符

2. URL过滤规则

URL 过滤功能实现的前提条件是对 URL 的识别。可通过使用 URL 过滤规则匹配 URL 中主机名字段和 URI 字段的方法来识别 URL。

URL 过滤规则是指对用户 HTTP 报文中的 URL 进行匹配的原则，且其分为两种规则：

- 预定义规则：根据设备中的 URL 过滤特征库自动生成，包括百万级的主机名或 URI。预定义规则能满足多数情况下的 URL 过滤需求。
- 自定义规则：由管理员手动配置生成，可以通过使用正则表达式或者文本的方式配置规则中主机名或 URI 的内容。

URL 过滤规则支持两种匹配方式：

- 文本匹配：使用指定的字符串对主机名和 URI 字段进行精确匹配。
  - 匹配主机名字段时，URL 中的主机名字段与规则中指定的主机名字符串必须完全一致，才能匹配成功。例如，规则中配置主机名字符串为 abc.com.cn，则主机名为 abc.com.cn 的 URL 会匹配成功，而主机名为 dfabc.com.cn 的 URL 将与该规则匹配失败。
  - 匹配 URI 字段时，从 URL 中 URI 字段的首字符开始，只要 URI 字段中连续若干个字符与规则中指定的 URI 字符串完全一致，就算匹配成功。例如，规则中配置 URI 字符串为 /sina/news，则 URI 为/sina/news、/sina/news/sports 或/sina/news_sports 的 URL 会匹配成功，而 URI 为/sina 的 URL 将与该规则匹配失败。
- 正则表达式匹配：使用正则表达式对主机名和 URI 字段进行模糊匹配。例如，规则中配置主机名的正则表达式为 sina.*cn，则主机名为 news.sina.com.cn 的 URL 会匹配成功。

3. URL过滤分类

为便于管理员对数目众多的 URL 过滤规则进行统一部署，URL 过滤模块提供了 URL 过滤分类功能，以便对具有相似特征的 URL 过滤规则进行归纳以及为匹配这些规则的 URL 统一指定处理动作。每个 URL 过滤分类具有一个严重级别属性，该属性值表示对属于此过滤分类 URL 的处理优先级。

URL 过滤分类包括两种类型：

- 预定义分类：根据设备中的 URL 过滤特征库自动生成，其严重级别不可被修改。
- 自定义分类：由管理员手动配置，可修改其严重级别，可添加 URL 过滤规则。

4. URL过滤策略

URL 过滤策略是用于关联所有 URL 过滤配置的一个实体。一个 URL 过滤策略中可以配置 URL 过滤分类和处理动作的绑定关系，以及缺省动作（即对未匹配上任何 URL 过滤规则的报文采取的动作）。URL 过滤支持的处理动作包括，丢弃、允许、阻断、重置、重定向和生成日志。

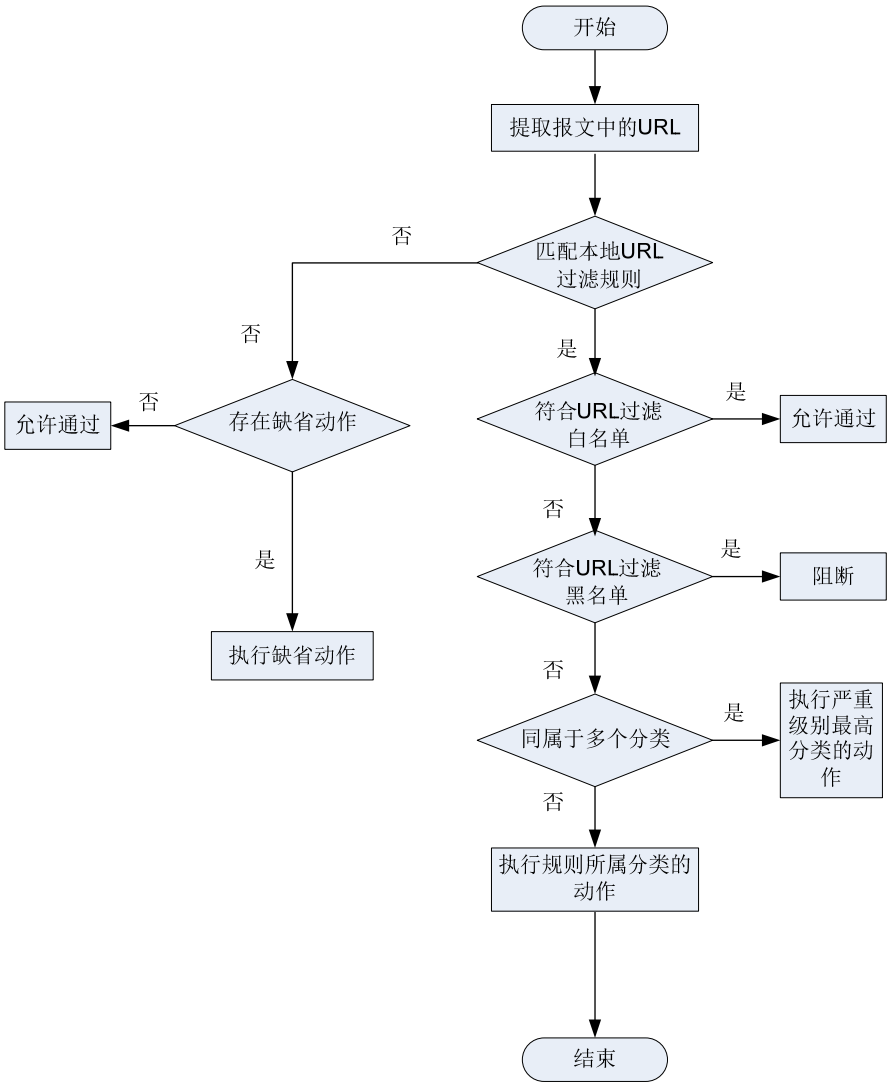
5. URL过滤黑/白名单规则

URL 过滤黑/白名单规则功能根据应用层的信息进行 URL 过滤。如果用户 HTTP 报文中的 URL 与 URL 过滤策略中的黑名单规则匹配成功，则丢弃此报文；如果与白名单规则匹配成功，则允许此报文通过。

1.1.2 URL过滤实现流程

在开启URL过滤功能的情况下，当用户通过设备使用HTTP访问某个网络资源时，设备将对此HTTP报文进行URL过滤。URL过滤处理流程如 图 1-2 所示：

图1-2 URL 过滤实现流程图



URL 过滤实现流程如下：

(1) 设备将提取报文的 URL 字段，并与 URL 过滤规则进行匹配。

(2) 设备将报文与 URL 过滤策略中的过滤规则进行匹配，如果匹配成功，则进行下一步处理；如果匹配失败，则进入步骤（5）的处理。

(3) 首先判断此 URL 过滤规则是否属于 URL 过滤的黑/白名单规则，如果属于 URL 过滤白名单规则则直接允许此报文通过，如果属于 URL 过滤的黑名单规则则直接将此报文阻断。

(4) 如果此 URL 过滤规则既不属于 URL 过滤白名单规则也不属于 URL 过滤黑名单规则，则设备将进一步判断该规则是否同时属于多个 URL 过滤分类。

- 如果此 URL 过滤规则同时属于多个 URL 过滤分类，则根据严重级别最高的 URL 过滤分类的动作对此报文进行处理。

- 如果此 URL 过滤规则只属于一个 URL 过滤分类，则根据该规则所属的 URL 过滤分类的动作对此报文进行处理。

(5) 如果设备上配置了 URL 过滤的缺省动作，则根据配置的缺省动作对此报文进行处理；否则直接允许报文通过。

1.1.3 URL过滤特征库升级与回滚

URL 过滤特征库是用来对经过设备的用户访问 Web 请求中的 URL 进行识别的资源库。随着互联网业务的不断变化和发展，需要及时升级设备中的 URL 过滤特征库，同时设备也支持 URL 过滤特征库回滚功能。

1. URL过滤特征库升级

URL 过滤特征库的升级包括如下几种方式：

- 定期自动在线升级：设备根据管理员设置的时间定期自动更新本地的 URL 过滤特征库。
- 立即自动在线升级：管理员手工触发设备立即更新本地的 URL 过滤特征库。
- 手动离线升级：当设备无法自动获取 URL 过滤特征库时，需要管理员先手动获取最新的 URL 过滤特征库，再更新本地的 URL 过滤特征库。

2. URL过滤特征库回滚

如果管理员发现设备当前 URL 过滤特征库对用户访问 Web 的 URL 过滤的误报率较高或出现异常情况，则可以将其回滚到出厂版本和上一版本。

1.2 URL过滤配置任务简介

表1-2 URL 过滤配置任务简介

配置任务	说明	详细配置
配置URL过滤分类	必选	1.3.1
配置URL过滤策略	必选	1.3.2
复制URL过滤策略或分类	可选	1.3.3
在DPI应用profile中引用URL过滤策略	必选	1.3.4
配置URL过滤特征库升级和回滚	可选	1.3.5
激活DPI各业务模块的策略和规则配置	可选	1.3.6
开启URL过滤日志信息功能	可选	1.3.7

1.3 配置URL过滤

1.3.1 配置URL过滤分类

当 URL 过滤特征库中预定义的 URL 过滤分类和 URL 过滤规则不能满足对 URL 的控制需求时，可以配置 URL 过滤分类，并在分类中创建 URL 过滤规则。每个 URL 过滤规则可以同时属于多个 URL 过滤分类。

不同 URL 过滤分类的严重级别不能相同，数值越大表示严重级别越高。

系统为预定义 URL 过滤分类保留的严重级别为最低，取值范围为 1～999。

表1-3 配置 URL 过滤分类

操作	命令	说明
进入系统视图	**system-view**	-
创建URL过滤分类，并进入URL过滤分类视图	**url-filter category** *category-name* [**severity** *severity-level*]	缺省情况下，只存在预定义的URL过滤分类，且分类名称以字符串Pre-开头 自定义的URL过滤分类不能以字符串Pre-开头
（可选）配置URL过滤分类的描述信息	**description** *text*	缺省情况下，自定义的URL过滤分类中不存在描述信息
配置自定义URL过滤规则	**rule** *rule-id* **host** { **regex** *regex* | **text** *string* } [**uri** { **regex** *regex* | **text** *string* }]	缺省情况下，URL过滤分类中不存在自定义URL过滤规则
（可选）添加预定义URL过滤分类中的规则	**include pre-defined** *category-name*	缺省情况下，URL过滤分类中未添加预定义URL过滤分类中的规则
（可选）重命名URL过滤分类，并进入新的URL过滤分类视图	**rename** *new-name*	-

1.3.2 配置URL过滤策略

在一个 URL 过滤策略中可以配置多个 URL 过滤分类动作，也可以在 URL 过滤策略中为其定义缺省动作。

若报文成功匹配的 URL 过滤规则同属于多个 URL 过滤分类，则根据严重级别最高的 URL 过滤分类中指定的动作对此报文进行处理。

表1-4 配置 URL 过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
创建URL过滤策略，并进入URL过滤策略视图	**url-filter policy** *policy-name*	缺省情况下，不存在URL过滤策略
配置URL过滤分类动作	**category** *category-name* **action** { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging**]	缺省情况下，不存在URL过滤分类动作
（可选）配置URL过滤策略的缺省动作	**default-action** { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging**]	缺省情况下，不存在缺省动作

操作	命令	说明
（可选）向URL过滤策略中添加黑/白名单规则	**add** { **blacklist** | **whitelist** } [*id*] **host** { **regex** *host-regex* | **text** *host-name* } [**uri** { **regex** *uri-regex* | **text** *uri-name* }]	缺省情况下，不存在黑/白名单规则
（可选）重命名URL过滤策略，并进入新的URL过滤策略视图	**rename** *new-name*	-

1.3.3 复制URL过滤策略或分类

此功能用来复制已存在的 URL 过滤策略或分类，可以方便用户快速创建 URL 过滤策略或分类。在复制 URL 过滤分类时，如果指定优先级与已经存在的分类优先级相同，则复制失败。

表1-5 复制 URL 过滤策略或分类

操作	命令	说明
进入系统视图	**system-view**	-
复制URL过滤分类	**url-filter copy category** *old-name new-name* **severity** *severity-level*	-
复制URL过滤策略	**url-filter copy policy** *old-name new-name*	-

1.3.4 在DPI应用profile中引用URL过滤策略

DPI 应用 porfile 是一个安全业务的配置模板，为实现 URL 过滤功能，必须在 DPI 应用 porfile 中引用指定的 URL 过滤策略。一个 DPI 应用 profile 中只能引用一个 URL 过滤策略，如果重复配置，则后配置的覆盖已有的。

表1-6 在 DPI 应用 profile 下引用 URL 过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
进入DPI应用profile视图	**app-profile** *app-profile-name*	-
在DPI应用profile中引用URL过滤策略	**url-filter apply policy** *policy-name*	缺省情况下，DPI应用profile中未引用URL过滤策略

1.3.5 配置URL过滤特征库升级和回滚

注意

- 请勿删除设备存储介质根目录下的/dpi/文件夹，否则设备升级或回滚特征库会失败。
- 当系统内存使用状态处于告警门限状态时，请勿进行特征库升级或回滚，否则易造成设备特征库升级或回滚失败，进而影响 URL 过滤业务的正常运行。有关内存告警门限状态的详细介绍请参见“基础配置指导”中的“设备管理”。

随着互联网业务的不断变化和发展，管理员需要及时升级设备中的 URL 过滤特征库，同时设备也支持 URL 过滤特征库回滚功能。

1. 配置定期自动在线升级URL过滤特征库

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 URL 过滤特征库进行升级。

说明

该方式下，需要确保设备能通过静态或动态域名解析方式获得官方网站的 IP 地址，并与之路由可达，否则设备升级 URL 过滤特征库会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

表1-7 配置定期自动在线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
开启定期自动在线升级URL过滤特征库功能，并进入自动在线升级配置视图	**url-filter signature auto-update**	缺省情况下，定期自动在线升级URL过滤特征库功能处于关闭状态
配置定期自动在线升级URL过滤特征库的时间	**update schedule** { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*	缺省情况下，设备在每天01:00:00至03:00:00之间自动升级URL过滤特征库

2. 立即自动在线升级URL过滤特征库

当管理员发现官方网站上的特征库服务专区中的 URL 过滤特征库有更新时，可以选择立即自动在线升级方式来及时升级 URL 过滤特征库版本。

说明

该方式下，需要确保设备能通过静态或动态域名解析方式获得官方网站的 IP 地址，并与之路由可达，否则设备升级 URL 过滤特征库会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

表1-8 立即自动在线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
立即自动在线升级URL过滤特征库	**url-filter signature auto-update-now**	-

3. 手动离线升级URL过滤特征库

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 URL 过滤特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 URL 过滤特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 URL 过滤特征库版本。

表1-9 手动离线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
手动离线升级URL过滤特征库	**url-filter signature update** *file-path*	-

4. 回滚URL过滤特征库

URL 过滤特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 URL 过滤特征库版本是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

表1-10 回滚 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
回滚URL过滤特征库	**url-filter signature rollback** { **factory** | **last** }	-

1.3.6 激活DPI各业务模块的策略和规则配置

当DPI各业务模块的策略和规则被创建、修改和删除后，需要配置此功能使其策略和规则配置生效。配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一配置此功能。

表1-11 激活 DPI 各业务模块的策略和规则配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略和规则	**inspect activate**	缺省情况下，DPI各业务模块的策略

操作	命令	说明
配置		和规则被创建、修改和删除时不生效

1.3.7 开启应用层检测引擎日志信息功能

应用层检测引擎日志是为了满足管理员审计需求。设备生成应用层检测引擎日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

表1-12 开启应用层检测引擎日志信息功能

操作	命令	说明
进入系统视图	**system-view**	-
开启应用层检测引擎日志信息功能	**url-filter log enable**	缺省情况下，生成应用层检测引擎日志信息功能处于关闭状态

1.4 URL过滤显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示 URL 过滤的配置信息和分类信息等。在用户视图下执行 **reset** 命令可以清除 URL 过滤的统计信息。

表1-13 URL 过滤显示和维护

操作	命令
显示URL过滤分类信息	**display url-filter category** [**verbose**]
显示URL过滤特征库信息	**display url-filter signature information**
查看URL过滤的统计信息	**display url-filter statistics**
清除URL过滤的统计信息	**reset url-filter statistics**