

# 目 录

1 Web过滤配置命令 .....	1-1
1.1 Web过滤配置命令 .....	1-1
1.1.1 display firewall http activex-blocking .....	1-1
1.1.2 display firewall http java-blocking .....	1-2
1.1.3 display firewall http url-filter host .....	1-4
1.1.4 display firewall http url-filter parameter.....	1-5
1.1.5 firewall http activex-blocking acl.....	1-7
1.1.6 firewall http activex-blocking enable.....	1-8
1.1.7 firewall http activex-blocking suffix .....	1-8
1.1.8 firewall http java-blocking acl.....	1-9
1.1.9 firewall http java-blocking enable .....	1-10
1.1.10 firewall http java-blocking suffix.....	1-10
1.1.11 firewall http url-filter host acl.....	1-11
1.1.12 firewall http url-filter host default.....	1-12
1.1.13 firewall http url-filter host enable.....	1-12
1.1.14 firewall http url-filter host ip-address.....	1-13
1.1.15 firewall http url-filter host url-address .....	1-13
1.1.16 firewall http url-filter parameter .....	1-15
1.1.17 firewall http url-filter parameter enable.....	1-16
1.1.18 reset firewall http .....	1-16

# 1 Web过滤配置命令

## 1.1 Web过滤配置命令

### 1.1.1 display firewall http activex-blocking

#### 【命令】

```
display firewall http activex-blocking [ all | item keywords | verbose ] [ [ { begin | exclude | include } regular-expression ]
```

#### 【视图】

任意视图

#### 【缺省级别】

1: 监控级

#### 【参数】

**all:** 显示所有阻断后缀关键字的相关信息。

**item keywords:** 显示指定阻断后缀关键字的相关信息。其中，*keywords* 表示阻断后缀关键字，为 1~9 个字符的字符串，不区分大小写。该字符串必须以“.”开头，且“.”之后的字符只能为数字或英文字母。

**verbose:** 显示 ActiveX 阻断的详细信息。

**|:** 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

**begin:** 从包含指定正则表达式的行开始显示。

**exclude:** 只显示不包含指定正则表达式的行。

**include:** 只显示包含指定正则表达式的行。

**regular-expression:** 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

#### 【描述】

**display firewall http activex-blocking** 命令用于显示 ActiveX 阻断信息。

如果不指定任何关键字，则显示 ActiveX 阻断的简要信息。

#### 【举例】

# 显示 ActiveX 阻断的简要信息。

```
<Sysname> display firewall http activex-blocking
```

```
ActiveX blocking is enabled.
```

以上显示信息表示 ActiveX 阻断功能已使能。

# 显示 ActiveX 阻断后缀关键字的相关信息。

```
<Sysname> display firewall http activex-blocking item .ocx
```

```
The HTTP request packet including ".ocx" had been matched for 5 times.
```

以上显示信息表示包含“.ocx”后缀的 ActiveX 请求报文已经匹配了 5 次。

# 显示所有 ActiveX 阻断后缀关键字的信息。

```
<Sysname> display firewall http activex-blocking all
SN    Match-Times    Keywords
-----
1     5                .OCX
2     0                .vbs
```

表1-1 display firewall http activex-blocking all 命令显示信息描述表

字段	描述
SN	条目序号
Match-Times	匹配的次數
Keywords	ActiveX 阻断后缀关键字

# 显示 ActiveX 阻断的详细信息。

```
<Sysname> display firewall http activex-blocking verbose
ActiveX blocking is enabled.
No ACL group has been configured.
There are 5 packet(s) being filtered.
There are 0 packet(s) being passed.
```

表1-2 display firewall http activex-blocking verbose 命令显示信息描述表

字段	描述
ActiveX blocking is enabled	ActiveX 阻断功能已使能
No ACL group has been configured	未设置 ACL 规则
There are 5 packet(s) being filtered	被阻断的报文数目
There are 0 packet(s) being passed	允许通过的报文数目

## 1.1.2 display firewall http java-blocking

### 【命令】

```
display firewall http java-blocking [ all | item keywords | verbose ] [ [ { begin | exclude | include } regular-expression ]
```

### 【视图】

任意视图

### 【缺省级别】

1: 监控级

### 【参数】

**all:** 显示所有阻断后缀关键字的相关信息。

**item keywords:** 显示指定阻断后缀关键字的相关信息。其中，*keywords* 表示阻断后缀关键字，为 1~9 个字符的字符串，不区分大小写。该字符串必须以“.”开头，且“.”之后的字符只能为数字或英文字母。

**verbose:** 显示 Java Applet 阻断的详细信息。

**|:** 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

**begin:** 从包含指定正则表达式的行开始显示。

**exclude:** 只显示不包含指定正则表达式的行。

**include:** 只显示包含指定正则表达式的行。

**regular-expression:** 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

### 【描述】

**display firewall http java-blocking** 命令用于显示 Java Applet 阻断信息。

如果不指定任何关键字，则显示 Java Applet 阻断的简要信息。

### 【举例】

# 显示 Java Applet 阻断的简要信息。

```
<Sysname> display firewall http java-blocking
Java blocking is enabled.
```

以上显示信息表示 Java Applet 阻断功能已使能。

# 显示指定 Java Applet 阻断后缀关键字的信息。

```
<Sysname> display firewall http java-blocking item .class
The HTTP request packet including ".class" had been matched for 10 times.
```

以上显示信息表示包含“.class”后缀的 Java Applet 请求报文已经匹配了 10 次。

# 显示所有 Java Applet 阻断后缀关键字的信息。

```
<Sysname> display firewall http java-blocking all
SN    Match-Times    Keywords
-----
1      10              .CLASS
2       0               .JAR
3       0               .java
```

表1-3 display firewall http java-blocking all 命令显示信息描述表

字段	描述
SN	条目序号
Match-Times	匹配的次数
Keywords	Java Applet 阻断后缀关键字

# 显示 Java Applet 阻断的详细信息。

```
<Sysname> display firewall http java-blocking verbose
Java blocking is enabled.
No ACL group has been configured.
There are 10 packet(s) being filtered.
There are 0 packet(s) being passed.
```

表1-4 display firewall http java-blocking verbose 命令显示信息描述表

字段	描述
Java blocking is enabled	Java 阻断功能已使能
No ACL group has been configured	未设置 ACL 规则
There are 10 packet(s) being filtered	被阻断的报文数目
There are 0 packet(s) being passed	允许通过的报文数目

### 1.1.3 display firewall http url-filter host

#### 【命令】

```
display firewall http url-filter host [ all | item keywords | verbose ] [ [ { begin | exclude | include } regular-expression ]
```

#### 【视图】

任意视图

#### 【缺省级别】

1: 监控级

#### 【参数】

**all:** 显示所有过滤关键字的相关信息。

**item *keywords*:** 显示指定过滤关键字的相关信息。其中，*keywords* 表示过滤关键字，为 1~80 个字符的字符串，不区分大小写，只能由数字、英文字母、通配符（“^”、“\$”、“&”和“\*”）以及它们的有限组合构成。

**verbose:** 显示网站地址过滤的详细信息。

**|:** 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

**begin:** 从包含指定正则表达式的行开始显示。

**exclude:** 只显示不包含指定正则表达式的行。

**include:** 只显示包含指定正则表达式的行。

***regular-expression*:** 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

#### 【描述】

**display firewall http url-filter host** 命令用于显示网站地址过滤信息。

如果不指定任何关键字，则显示网站地址过滤的简要信息。

#### 【举例】

# 显示网站地址过滤的简要信息。

```
<Sysname> display firewall http url-filter host
URL-filter host is enabled.
Default method: permit.
```

以上显示信息表示网站地址过滤功能已使能，缺省的过滤行为允许 Web 请求通过。

# 显示指定网站地址过滤条目的信息。

```
<Sysname> display firewall http url-filter host item ^webfilter$
The HTTP request packet including "^webfilter$" had been matched for 10 times.
```

# 显示所有网站地址过滤条目的信息。

```
<Sysname> display firewall http url-filter host all
SN      Match-Times  Keywords
-----
1        10             ^webfilter$
```

表1-5 display firewall http url-filter host all 命令显示信息描述表

字段	描述
SN	条目序号
Match-Times	匹配的次數
Keywords	网站地址过滤关键字

# 显示网站地址过滤的详细信息。

```
<Sysname> display firewall http url-filter host verbose
URL-filter host is enabled.
Default method: permit.
The support for IP address: deny.
No ACL group has been configured.
There are 10 packet(s) being filtered.
There are 0 packet(s) being passed.
```

表1-6 display firewall http url-filter host verbose 命令显示信息描述表

字段	描述
URL-filter host is enabled	网站地址过滤功能已使能
Default method	缺省的过滤行为，取值包括 permit 和 deny
The support for IP address	对网站 IP 地址的支持情况，取值包括 permit 和 deny
No ACL group has been configured.	未设置 ACL 规则
There are 10 packet(s) being filtered	被阻断的报文数目
There are 0 packet(s) being passed	允许通过的报文数目

## 1.1.4 display firewall http url-filter parameter

### 【命令】

```
display firewall http url-filter parameter [ all | item keywords | verbose ] [ { begin | exclude | include } regular-expression ]
```

### 【视图】

任意视图

## 【缺省级别】

1: 监控级

## 【参数】

**all:** 显示所有过滤参数的相关信息。

**item keywords:** 显示指定过滤参数的相关信息。其中, *keywords* 表示过滤参数, 为 1~80 个字符的字符串, 不区大小写, 只能由数字、英文字母、通配符 (“^”、“\$”、“&”和“\*”) 以及其它 ASCII 字符 (31<ASCII 值<127) 构成。

**verbose:** 显示 URL 参数过滤的详细信息。

**|:** 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍, 请参见“基础配置指导”中的“CLI”。

**begin:** 从包含指定正则表达式的行开始显示。

**exclude:** 只显示不包含指定正则表达式的行。

**include:** 只显示包含指定正则表达式的行。

**regular-expression:** 表示正则表达式, 为 1~256 个字符的字符串, 区分大小写。

## 【描述】

**display firewall http url-filter parameter** 命令用于显示 URL 参数过滤信息。

如果不指定任何关键字, 则显示 URL 参数过滤的简要信息。

## 【举例】

# 显示 URL 参数过滤的简要信息。

```
<Sysname> display firewall http url-filter parameter
URL-filter parameter is enabled.
```

以上显示信息表示 URL 参数过滤功能已使能。

# 显示指定 URL 过滤参数的信息。

```
<Sysname> display firewall http url-filter parameter item ^select$
The HTTP request packet including "^select$" had been matched for 10 times.
```

以上显示信息表示包含 “^select\$” 过滤参数的 HTTP 请求报文已经匹配了 10 次。

# 显示所有 URL 过滤参数的信息。

```
<Sysname> display firewall http url-filter parameter all
SN      Match-Times  Keywords
-----
1       0            ^select$
2       0            ^insert$
3       0            ^update$
4       0            ^delete$
5       0            ^drop$
6       0            --
7       0            `
8       0            ^exec$
9       10         %27
10      0            qqpppp
```

表1-7 display firewall http url-filter parameter all 命令显示信息描述表

字段	描述
SN	条目序号
Match-Times	匹配的次數
Keywords	URL 过滤参数关键字

# 显示 URL 参数过滤的详细信息。

```
<Sysname> display firewall http url-filter parameter verbose
URL-filter parameter is enabled.
There are 10 packet(s) being filtered.
There are 0 packet(s) being passed.
```

表1-8 display firewall http url-filter parameter verbose 命令显示信息描述表

字段	描述
URL-filter parameter is enabled	URL 参数过滤功能已使能
There are 10 packet(s) being filtered	被阻断的报文数目
There are 0 packet(s) being passed	允许通过的报文数目

## 1.1.5 firewall http activex-blocking acl

### 【命令】

```
firewall http activex-blocking acl acl-number
undo firewall http activex-blocking acl
```

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

*acl-number*: ACL 的编号，取值范围为 2000~3999。

### 【描述】

**firewall http activex-blocking acl** 命令用来设置 ActiveX 阻断的 ACL 规则。**undo firewall http activex-blocking acl** 命令用来删除设置的 ActiveX 阻断 ACL 规则。

缺省情况下，未设置 ActiveX 阻断的 ACL 规则。

需要注意的是：

- 该命令生效后，所有 URL 中带有 ActiveX 阻断关键字列表中列出的后缀关键字的 Web 请求将按照 ACL 规则规定的方式进行处理。
- 可多次设置 ACL，但仅最后一次合法的配置生效。



- 若设置的 ACL 不存在，该配置可以成功，但是根据 ACL 过滤 ActiveX 的功能暂时不生效，直到该 ACL 配置后才能生效。

相关配置可参考命令 **display firewall http activex-blocking**。

#### 【举例】

```
# 指定 ActiveX 阻断的 ACL 为 ACL 2003。  
<Sysname> system-view  
[Sysname] firewall http activex-blocking acl 2003
```

### 1.1.6 firewall http activex-blocking enable

#### 【命令】

```
firewall http activex-blocking enable  
undo firewall http activex-blocking enable
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

无

#### 【描述】

**firewall http activex-blocking enable** 命令用来使能 ActiveX 阻断功能，并将缺省阻断关键字 “.ocx” 添加到 ActiveX 阻断关键字列表中。**undo firewall http activex-blocking enable** 命令用来关闭 ActiveX 阻断功能。

缺省情况下，ActiveX 阻断功能处于关闭状态。

相关配置可参考命令 **display firewall http activex-blocking**。

#### 【举例】

```
# 使能 ActiveX 阻断功能。  
<Sysname> system-view  
[Sysname] firewall http activex-blocking enable
```

### 1.1.7 firewall http activex-blocking suffix

#### 【命令】

```
firewall http activex-blocking suffix keywords  
undo firewall http activex-blocking suffix keywords
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

### 【参数】

**keywords:** 表示需要阻断的后缀关键字，为 1~9 个字符的字符串，不区分大小写。该字符串必须以 “.” 开头，且 “.” 之后的字符只能为数字或英文字母。

### 【描述】

**firewall http activex-blocking suffix** 命令用来添加 ActiveX 阻断后缀关键字。**undo firewall http activex-blocking suffix** 命令用来将指定的 ActiveX 阻断后缀关键字从 ActiveX 阻断关键字列表中删除。

需要注意的是：

- 最多允许添加 5 个 ActiveX 阻断后缀关键字。
- 不能使用该命令添加缺省的阻断后缀关键字 “.ocx”，同样，也不能使用 **undo** 命令来删除 “.ocx”。

相关配置可参考命令 **display firewall http activex-blocking**。

### 【举例】

# 将.vbs 添加到 ActiveX 阻断关键字列表中。

```
<Sysname> system-view  
[Sysname] firewall http activex-blocking suffix .vbs
```

## 1.1.8 firewall http java-blocking acl

### 【命令】

**firewall http java-blocking acl *acl-number***

**undo firewall http java-blocking acl**

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

**acl-number:** ACL 的编号，取值范围为 2000~3999。

### 【描述】

**firewall http java-blocking acl** 命令用来设置 Java Applet 阻断的 ACL 规则。**undo firewall http java-blocking acl** 命令用来删除设置的 Java Applet 阻断 ACL 规则。

缺省情况下，未设置 Java Applet 阻断的 ACL 规则。

需要注意的是：

- 该命令生效后，所有 URL 中带有 Java Applet 阻断关键字列表中列出的后缀关键字的 Web 请求将按照 ACL 规则规定的方式进行处理。
- 可多次设置 ACL，但仅最后一次合法的配置生效。
- 若设置的 ACL 不存在，该配置可以成功，但是根据 ACL 过滤 Java Applet 的功能暂时不生效，直到该 ACL 规则配置后才能生效。

相关配置可参考命令 **display firewall http java-blocking**。

### 【举例】

```
# 指定 Java Applet 阻断的 ACL 为 ACL 2002。
<Sysname> system-view
[Sysname] firewall http java-blocking acl 2002
```

## 1.1.9 firewall http java-blocking enable

### 【命令】

```
firewall http java-blocking enable
undo firewall http java-blocking enable
```

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

无

### 【描述】

**firewall http java-blocking enable** 命令用来使能 Java Applet 阻断功能，并将缺省阻断后缀关键字 “.class” 和 “.jar” 添加到 Java 阻断关键字列表中。**undo firewall http java-blocking enable** 命令用来关闭 Java Applet 阻断功能。

缺省情况下，Java Applet 阻断功能处于关闭状态。

相关配置可参考命令 **display firewall http java-blocking**。

### 【举例】

```
# 使能 Java Applet 阻断功能。
<Sysname> system-view
[Sysname] firewall http java-blocking enable
```

## 1.1.10 firewall http java-blocking suffix

### 【命令】

```
firewall http java-blocking suffix keywords
undo firewall http java-blocking suffix keywords
```

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

**keywords**: 表示需要阻断的后缀关键字，为 1~9 个字符的字符串，不区分大小写。该字符串必须以 “.” 开头，且 “.” 之后的字符只能为数字或英文字母。

### 【描述】

**firewall http java-blocking suffix** 命令用来添加 Java Applet 阻断后缀关键字。**undo firewall http java-blocking suffix** 命令用来将指定的 Java Applet 阻断后缀关键字从 Java Applet 阻断关键字列表中删除。

需要注意的是：

- 最多允许添加 5 个 Java Applet 阻断后缀关键字。
- 不能使用 **undo** 命令删除缺省的阻断后缀关键字 “.class” 和 “.jar”。

相关配置可参考命令 **display firewall http java-blocking**。

### 【举例】

```
# 将.js 添加到 Java Applet 阻断后缀关键字列表中。  
<Sysname> system-view  
[Sysname] firewall http java-blocking suffix .js
```

## 1.1.11 firewall http url-filter host acl

### 【命令】

**firewall http url-filter host acl *acl-number***  
**undo firewall http url-filter host acl**

### 【视图】

系统视图

### 【缺省级别】

2：系统级

### 【参数】

*acl-number*：ACL 的编号，取值范围为 2000~3999。

### 【描述】

**firewall http url-filter host acl** 命令用来设置网站地址过滤的 ACL 规则。**undo firewall http url-filter host acl** 命令用来删除设置的网站地址过滤 ACL 规则。

缺省情况下，未设置网站地址过滤的相关 ACL 规则。

需要注意的是：

- 该命令配置后，将按照设置的 ACL 规则对所有以网站 IP 地址直接访问网站的 Web 请求进行过滤。
- 可多次设置 ACL，但仅最后一次合法的配置生效。
- 若设置的 ACL 不存在，该配置可以成功，但是根据 ACL 过滤网站的功能暂时不生效，直到该 ACL 规则配置后才能生效。

相关配置可参考命令 **display firewall http url-filter host**。

### 【举例】

```
# 指定网站地址过滤的 ACL 规则，仅允许网站 IP 地址符合 ACL 2000 的 Web 请求通过。  
<Sysname> system-view  
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] rule 0 permit source 3.3.3.3 0.0.0.0
[Sysname-acl-basic-2000] quit
[Sysname] firewall http url-filter host acl 2000
```

### 1.1.12 firewall http url-filter host default

#### 【命令】

```
firewall http url-filter host default { deny | permit }
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**deny:** 表示拒绝 Web 请求通过。

**permit:** 表示允许 Web 请求通过。

#### 【描述】

**firewall http url-filter host default** 命令用来配置网站地址过滤的缺省过滤行为，即当 Web 请求中的 URL 与网站过滤地址列表中的条目不匹配时，允许或拒绝该请求通过。

缺省情况下，缺省的过滤行为为 **deny**。

相关配置可参考命令 **display firewall http url-filter host**。

#### 【举例】

# 设置网站地址过滤的缺省过滤行为为允许。

```
<Sysname> system-view
[Sysname] firewall http url-filter host default permit
```

### 1.1.13 firewall http url-filter host enable

#### 【命令】

```
firewall http url-filter host enable
undo firewall http url-filter host enable
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

无

#### 【描述】

**firewall http url-filter host enable** 命令用来使能网站地址过滤功能。**undo firewall http url-filter host enable** 命令用来关闭网站地址过滤功能。

缺省情况下，网站地址过滤功能处于关闭状态。

相关配置可参考命令 **display firewall http url-filter host**。

#### 【举例】

# 使能网站地址过滤功能。

```
<Sysname> system-view
[Sysname] firewall http url-filter host enable
```

### 1.1.14 firewall http url-filter host ip-address

#### 【命令】

**firewall http url-filter host ip-address { deny | permit }**

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**deny**: 拒绝目标 URL 为 IP 地址的 Web 请求通过。

**permit**: 允许目标 URL 为 IP 地址的 Web 请求通过。

#### 【描述】

**firewall http url-filter host ip-address** 命令用来配置网站地址过滤对网站 IP 地址的支持，即允许或拒绝以网站 IP 地址直接访问网站的 Web 请求。

缺省情况下，网站地址过滤不支持网站 IP 地址，即拒绝以网站 IP 地址直接访问网站的 Web 请求通过。

本配置在网站地址过滤功能使能后生效。

相关配置可参考命令 **firewall http url-filter host enable** 和 **display firewall http url-filter host**。

#### 【举例】

# 配置允许以网站 IP 地址直接访问网站的 Web 请求通过。

```
<Sysname> system-view
[Sysname] firewall http url-filter host ip-address permit
```

### 1.1.15 firewall http url-filter host url-address

#### 【命令】

**firewall http url-filter host url-address { deny | permit } url-address**

**undo firewall http url-filter host url-address [ url-address ]**

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

## 【参数】

**deny**: 表示过滤行为为拒绝。

**permit**: 表示过滤行为为允许。

**url-address**: 表示网站过滤地址条目（URL地址），为 1~80 个字符的字符串，不区分大小写，只能由数字、英文字母、“.”、“-”、“\_”、通配符（“^”、“\$”、“&”和“\*”）以及它们的有限组合构成。通配符具体含义如表 1-9 所示：

表1-9 通配符含义

通配符	含义	使用说明
^	表明是开头匹配	只能出现在过滤关键字的开头，且只能出现一次
\$	表明是结尾匹配	只能出现在过滤关键字的结尾，且只能出现一次
&	代替一个字符，不能代替“.”	可出现任意多个，也可连续出现，可位于过滤关键字的任意位置，不能与“*”一起使用
*	可代替任意多个字符，也可代替空格，不能代替“.”	在过滤关键字中只能出现一次，可以位于过滤关键字的开头和中间，不能位于结尾，并且不能和“^”、“\$”相邻

通配符的使用还需遵从以下使用规则：

- 如果过滤关键字的开头有“^”或结尾有“\$”，表示精确匹配。例如，“^webfilter”表示以“webfilter”开头的网址（如 webfilter.com.cn）或“.”后字符以“webfilter”开头的网址（如 cmm.webfilter-any.com）将被过滤掉。关键字“^webfilter\$”表示过滤包含独立词语“webfilter”的网址，比如 www.webfilter.com，但是类似于 www.webfilter-china.com 的网址将不会被过滤；
- 如果过滤关键字的开头和结尾都没有通配符，表示模糊匹配。对于模糊匹配，只要网址中包含了该关键字就会被过滤；
- 当“\*”位于过滤关键字的开头时，必须以“\*.其它关键字”的形式出现，例如“\*.com”或者“\*.webfilter.com”；
- 不支持纯数字的过滤地址。如果需要过滤类似 www.123.com 的网站，使用“123”作为过滤地址是不合法的，但可以使用“^123\$”、“www.123.com”和“123.com”等作为过滤地址。因此，对于以数字作为网站地址的网站，建议采用精确匹配方式进行过滤。

## 【描述】

**firewall http url-filter host url-address** 命令用来添加网站地址过滤条目，并设置过滤行为。**undo firewall http url-filter host url-address** 命令用来删除网站地址过滤条目。

需要注意的是：

- 如果不指定 *url-address*，则 **undo** 命令将删除所有网站地址过滤条目。
- 系统最多允许添加 256 个过滤条目。
- 可以直接对已存在的过滤条目的过滤行为进行修改，例如，某过滤条目的行为为 **deny**，可以直接将其修改为 **permit**。

相关配置可参考命令 **display firewall http url-filter host**。

## 【举例】

# 将过滤条目^china&添加到过滤地址列表中，并设置过滤行为为允许。

```
<Sysname> system-view
[Sysname] firewall http url-filter host url-address permit ^china&
```

### 1.1.16 firewall http url-filter parameter

#### 【命令】

```
firewall http url-filter parameter { default | keywords keywords }
undo firewall http url-filter parameter [ default | keywords keywords ]
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**default:** 表示使用缺省过滤参数进行过滤。系统预定义的缺省过滤参数包括：`^select$`、`^insert$`、`^update$`、`^delete$`、`^drop$`、`--`、`'`、`^exec$`和`%27`。

**keywords keywords:** 表示使用自定义过滤参数进行过滤。其中，*keywords*表示需要过滤的URL参数关键字，为1~80个字符的字符串，不区分大小写，只能由数字、英文字母、通配符（“^”、“\$”、“&”和“\*”）以及其它ASCII字符（31<ASCII值<127）构成。配置的过滤参数支持带空格形式的参数，但该参数必须用“”括起来，如“select all”。一个空格可以匹配参数名中连续的多个空格。通配符具体含义如 [表 1-10](#)所示：

表1-10 通配符含义

通配符	含义	使用说明
^	表明是开头匹配	只能位于过滤关键字的开头，且只能出现一次
\$	表明是结尾匹配	只能位于过滤关键字的结尾，且只能出现一次
&	代替一个字符	可出现任意多个，也可连续出现，可位于过滤关键字的任意位置，但不能与“*”相邻，如果出现在开始和结尾的位置，则一定要和“^”或“\$”相邻
*	代替不超过4个任意字符，可代替空格	只能位于过滤关键字的中间，且只能出现一次

通配符的使用还需遵从以下使用规则：

- 如果关键字的开头有“^”或结尾有“\$”，表示精确匹配。例如，关键字“^webfilter\$”表示网址中的URL参数包含独立词语“webfilter”的请求将被过滤掉，比如www.abc.com/webfilter any，但是类似于www.abc.com/webfilterany的网址将不会被过滤。
- 如果关键字的开头和结尾都没有通配符，表示模糊匹配。对于模糊匹配，只要网址中的URL参数包含了该关键字就会被过滤。

#### 【描述】

**firewall http url-filter parameter** 命令用来添加URL过滤参数，即将指定的过滤参数添加到URL过滤参数列表中。**undo firewall http url-filter parameter** 命令用来删除URL过滤参数。

需要注意的是：



- 如果不指定任何参数，则 **undo** 命令将删除所有 URL 过滤参数。
- 包括缺省过滤参数在内，用户最多可添加 256 个过滤参数。
- **firewall http url-filter parameter keywords** 命令和 **undo firewall http url-filter parameter keywords** 命令中指定的 URL 过滤参数不能与缺省过滤参数相同。

相关配置可参考命令 **display firewall http url-filter parameter**。

#### 【举例】

# 将 select 添加到 URL 过滤参数列表中。

```
<Sysname> system-view
[Sysname] firewall http url-filter parameter keywords select
```

### 1.1.17 firewall http url-filter parameter enable

#### 【命令】

```
firewall http url-filter parameter enable
undo firewall http url-filter parameter enable
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

无

#### 【描述】

**firewall http url-filter parameter enable** 命令用来使能 URL 参数过滤功能。**undo firewall http url-filter parameter enable** 命令用来关闭 URL 参数过滤功能。

缺省情况下，URL 参数过滤功能处于关闭状态。

相关配置可参考命令 **display firewall http url-filter parameter**。

#### 【举例】

# 使能 URL 参数过滤功能。

```
<Sysname> system-view
[Sysname] firewall http url-filter parameter enable
```

### 1.1.18 reset firewall http

#### 【命令】

```
reset firewall http { activex-blocking | java-blocking | url-filter host | url-filter parameter } counter
```

#### 【视图】

用户视图

#### 【缺省级别】

1: 监控级

### 【参数】

**activex-blocking:** 清除 ActiveX 阻断的过滤统计信息。

**java-blocking:** 清除 Java Applet 阻断的过滤统计信息。

**url-filter host:** 清除网站地址过滤统计信息。

**url-filter parameter:** 清除 URL 参数过滤统计信息。

**counter:** 表示清除统计信息。

### 【描述】

**reset firewall http** 命令用来清除 Web 过滤统计信息。

### 【举例】

# 清除网站地址过滤的统计信息。

```
<Sysname> reset firewall http url-filter host counter
```