H3C SecPath U 系列安全产品

攻击防范命令参考

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6PW104-20111209
产品版本：SECPATH200US&200UCS&200UCM -CMW520-R5116P20
SECPATH200UA&200UM&200UCA -CMW520-R5116P20

H3C、  、Aolynk、  、H^{3}Care、  、TOP G、  、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C SecPath U 系列安全产品 命令参考共分为八本手册，介绍了 U 系列安全产品各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《攻击防范命令参考》主要介绍配置 ARP 攻击防御和 Web 过滤的相关命令。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 产品配套资料
- 资料获取方式
- 技术支持
- 资料意见反馈

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表U系列安全产品。
	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C SecPath U 系列安全产品的配套资料包括如下部分：

大类	资料名称		内容介绍
产品知识介绍	产品彩页	U200-A	帮助您了解产品的主要规格参数及亮点
		U200-M	
		U200-S	
		U200-CA	
		U200-CM	
		U200-CS	
	FAQ		帮助您快速了解产品的软/硬件规格和特点
硬件描述与安装	安装指导		帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	License激活申请和注册操作指导		帮助您详细了解申请和注册License，以便及时更新升级应用程序和特征库
	H3C 可插拔SFP[SFP+][XFP]模块安装指南		帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导		帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考		详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
	典型配置举例		帮助您了解产品的典型应用和推荐配置，从组网需求、组网图、配置步骤几方面进行介绍
运行维护	版本说明书	U200-A	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法
		U200-M	
		U200-S	
		U200-CA	
		U200-CM	
		U200-CS	

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ARP攻击防御 ····· 1-1
1.1 ARP防IP报文攻击配置命令 ····· 1-1
1.1.1 arp resolving-route enable ····· 1-1
1.2 源MAC地址固定的ARP攻击检测配置命令 ····· 1-1
1.2.1 arp anti-attack source-mac ····· 1-1
1.2.2 arp anti-attack source-mac aging-time ····· 1-2
1.2.3 arp anti-attack source-mac exclude-mac ····· 1-3
1.2.4 arp anti-attack source-mac threshold ····· 1-3
1.2.5 display arp anti-attack source-mac ····· 1-4
1.3 ARP报文源MAC一致性检查配置命令 ····· 1-5
1.3.1 arp anti-attack valid-ack enable ····· 1-5
1.4 ARP主动确认配置命令 ····· 1-5
1.4.1 arp anti-attack active-ack enable ····· 1-5
1.5 ARP Detection配置命令 ····· 1-6
1.5.1 arp detection enable ····· 1-6
1.5.2 arp detection mode ····· 1-7
1.5.3 arp detection static-bind ····· 1-7
1.5.4 arp detection trust ····· 1-8
1.5.5 arp detection validate ····· 1-8
1.5.6 arp restricted-forwarding enable ····· 1-9
1.5.7 display arp detection ····· 1-10
1.5.8 display arp detection statistics ····· 1-10
1.5.9 reset arp detection statistics ····· 1-11
1.6 ARP自动扫描、固化配置命令 ····· 1-12
1.6.1 arp fixup ····· 1-12
1.6.2 arp scan ····· 1-13

1 ARP攻击防御

1.1 ARP防IP报文攻击配置命令

1.1.1 arp resolving-route enable

【命令】

arp resolving-route enable

undo arp resolving-route enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp resolving-route enable 命令用来启用 ARP 防 IP 报文攻击功能。**undo arp resolving-route enable** 命令用来关闭 ARP 防 IP 报文攻击功能。

默认情况下关闭 ARP 防 IP 报文攻击功能。

【举例】

启用 ARP 防 IP 报文攻击功能。

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

1.2 源MAC地址固定的ARP攻击检测配置命令

1.2.1 arp anti-attack source-mac

【命令】

arp anti-attack source-mac { **filter** | **monitor** }

undo arp anti-attack source-mac [**filter** | **monitor**]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

filter：检测到攻击后，打印告警信息，同时对该源 MAC 地址对应的 ARP 报文进行过滤。

monitor：检测到攻击后，只打印告警信息，不对该源 MAC 地址对应的 ARP 报文进行过滤。

【描述】

arp anti-attack source-mac 命令用来使能源 MAC 地址固定 ARP 攻击检测功能，并选择检查模式。**undo arp anti-attack source-mac** 命令用来恢复缺省情况。

缺省情况下，源 MAC 固定 ARP 攻击检测功能处于关闭状态。

使能源 MAC 固定 ARP 攻击检测之后，该特性会对上送 CPU 的 ARP 报文按照源 MAC 和 VLAN 进行统计。当在一定时间（5 秒）内收到某固定源 MAC 地址的 ARP 报文超过设定的阈值，不同模式的处理方式存在差异：在 **filter** 模式下会打印告警信息并对该源 MAC 地址对应的 ARP 报文进行过滤；在 **monitor** 模式下只进行告警，不过滤 ARP 报文。

需要注意的是，如果 **undo** 命令中没有指定检查模式，则关闭任意检查模式的源 MAC 固定 ARP 攻击检测功能。

【举例】

使能源 MAC 固定 ARP 攻击检测功能，并选择 **filter** 检查模式。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac filter
```

1.2.2 arp anti-attack source-mac aging-time

【命令】

arp anti-attack source-mac aging-time *time*

undo arp anti-attack source-mac aging-time

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

time：源 MAC 地址固定的 ARP 攻击检测表项的老化时间，取值范围为 60～6000，单位为秒。

【描述】

arp anti-attack source-mac aging-time 命令用来配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。**undo arp anti-attack source-mac aging-time** 命令用来恢复缺省情况。

缺省情况下，源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒，即 5 分钟。

【举例】

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

1.2.3 arp anti-attack source-mac exclude-mac

【命令】

arp anti-attack source-mac exclude-mac *mac-address*&<1-n>

undo arp anti-attack source-mac exclude-mac [*mac-address*&<1-n>]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

mac-address&<1-n>：MAC 地址列表。其中，*mac-address* 表示配置的保护 MAC 地址，格式为 H-H-H。&<1-n>表示每次最多可以配置的保护 MAC 地址个数。n 的取值范围 1～10。

【描述】

arp anti-attack source-mac exclude-mac 命令用来配置保护 MAC。当配置了保护 MAC 之后，即使该 ARP 报文中的 MAC 地址存在攻击也不会被检测过滤。**undo arp anti-attack source-mac exclude-mac** 命令用来取消配置的保护 MAC。

缺省情况下，没有配置任何保护 MAC。

需要注意的是，如果 **undo** 命令中没有指定 MAC 地址，则取消所有配置的保护 MAC。

【举例】

配置源 MAC 固定攻击检查的保护 MAC 地址为 2-2-2。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

1.2.4 arp anti-attack source-mac threshold

【命令】

arp anti-attack source-mac threshold *threshold-value*

undo arp anti-attack source-mac threshold

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

threshold-value：固定时间内源 MAC 固定 ARP 报文攻击检测的阈值，单位为报文个数。取值范围 10～100，缺省值 50。

【描述】

arp anti-attack source-mac threshold 命令用来配置源 MAC 固定 ARP 报文攻击检测阈值，当在固定的时间（5 秒）内收到源 MAC 固定的 ARP 报文超过该阈值则认为存在攻击。**undo arp anti-attack source-mac threshold** 命令用来恢复缺省阈值。

【举例】

配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac threshold 30
```

1.2.5 display arp anti-attack source-mac

【命令】

display arp anti-attack source-mac [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface *interface-type interface-number*：显示指定接口检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【描述】

display arp anti-attack source-mac 命令用来显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

在集中式设备上，如果不指定接口，则显示所有接口检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【举例】

显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp anti-attack source-mac
Source-MAC          VLAN ID          Interface            Aging-time
23f3-1122-3344      4094             GE0/0                10
23f3-1122-3355      4094             GE0/1                30
23f3-1122-33ff      4094             GE0/2                25
23f3-1122-33ad      4094             GE0/3                30
23f3-1122-33ce      4094             GE0/4                2
```

表1-1 display arp anti-attack source-mac 命令显示信息描述表

字段	描述
Source-MAC	检测到攻击的源MAC地址
VLAN ID	检测到攻击的VLAN ID
Interface	攻击来源的接口索引
Aging-time	ARP防攻击策略表项老化剩余时间

1.3 ARP报文源MAC一致性检查配置命令

1.3.1 arp anti-attack valid-ack enable

【命令】

arp anti-attack valid-check enable

undo arp anti-attack valid-check enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp anti-attack valid-check enable 命令用来在网关设备上使能 ARP 报文源 MAC 一致性检查功能。网关使能此功能时，会对接收的 ARP 报文进行检查，如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则丢弃该报文。**undo arp anti-attack valid-check enable** 命令用来关闭 ARP 报文源 MAC 一致性检查功能。

缺省情况下，关闭 ARP 源 MAC 一致性检查功能。

【举例】

使能 ARP 源 MAC 一致性检查功能。

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

1.4 ARP主动确认配置命令

1.4.1 arp anti-attack active-ack enable

【命令】

arp anti-attack active-ack enable

undo arp anti-attack active-ack enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp anti-attack active-ack enable 命令用来使能 ARP 主动确认功能。**undo arp anti-attack active-ack enable** 命令用来恢复缺省情况。

缺省情况下，关闭 ARP 主动确认功能。

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

ARP 主动确认功能包括两部分：新建 ARP 表项前的主动确认、修改已有 ARP 表项前的主动确认。

- 新建 ARP 表项前的主动确认：当收到 ARP 报文触发新建动态 ARP 表项时，设备根据收到的 ARP 报文的源 IP 地址发送一个广播 ARP 请求报文，如果在随后的 3 秒内收到对应的 ARP 应答报文，则新建 ARP 表项。否则忽略之前收到 ARP 攻击报文，不新建 ARP 表项。
- 修改已有 ARP 表项前的主动确认：当收到的 ARP 报文中的源 MAC 地址和对应 ARP 表项中的不同时，首先判断 ARP 表项刷新时间是否超过 1 分钟，如果没有超过 1 分钟，则不更新 ARP 表项。否则向 ARP 表项对应的源发送一个单播请求，如果在随后的 5 秒内收到对应的应答报文，则忽略之前收到的 ARP 攻击报文；如果没有收到对应的应答报文，则向之前收到的 ARP 报文对应的源发送一个单播请求，如果在随后的 5 秒内收到了对应的应答报文，则根据该 ARP 报文更新 ARP 表项，否则 ARP 表项不会被修改。

【举例】

使能 ARP 主动确认功能。

```
<Sysname> system-view
[Sysname] arp anti-attack active-ack enable
```

1.5 ARP Detection配置命令

1.5.1 arp detection enable

【命令】

arp detection enable

undo arp detection enable

【视图】

VLAN 视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp detection enable 命令用来使能 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。**undo arp detection enable** 命令用来关闭 ARP Detection 功能。

缺省情况下，关闭 ARP Detection 功能。

【举例】

使能 ARP Detection 功能。

```
<Sysname> system-view
```

```
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

1.5.2 arp detection mode

【命令】

arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

undo arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dhcp-snooping：基于 DHCP Snooping 安全表项的检查模式，此模式主要针对仿冒用户的攻击。

dot1x：基于 802.1X 安全表项的检查模式，此模式主要针对仿冒用户的攻击。

static-bind：基于 IP 和 MAC 静态绑定表项的检查模式，此模式主要针对仿冒网关的攻击。

【描述】

arp detection mode 命令用来配置 ARP Detection 检查模式。**undo arp detection mode** 命令用来取消指定的 ARP Detection 检查模式。

缺省情况下，没有配置 ARP Detection 检查模式，认为所有报文都是非法的。

需要注意的是，如果同时配置了三种检查模式，则先进行 IP 和 MAC 静态绑定表项检查，然后进行 DHCP Snooping 安全表项检查，最后进行 802.1X 安全表项检查。

【举例】

配置 ARP Detection 基于 DHCP Snooping 表项和 802.1X 安全表项的检查模式。

```
<Sysname> system-view
[Sysname] arp detection mode dhcp-snooping
[Sysname] arp detection mode dot1x
```

1.5.3 arp detection static-bind

【命令】

arp detection static-bind *ip-address mac-address*

undo arp detection static-bind [*ip-address*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：静态绑定表项的 IP 地址部分。

mac-address：静态绑定表项的 MAC 地址部分，格式为 H-H-H。

【描述】

arp detection static-bind 命令用来配置 IP 和 MAC 的静态绑定表项。**undo arp detection static-bind** 命令用来删除已经配置的 IP 和 MAC 的静态绑定表项。

缺省情况下，没有静态绑定表项。

对于源 IP 存在绑定关系但是 MAC 地址不符的 ARP 报文，设备认为是非法报文进行丢弃处理；对于源 IP 不存在绑定关系和源 IP 存在绑定关系且 MAC 地址相符的 ARP 报文，设备认为是合法报文，通过检查。

需要注意的是，如果 **undo** 命令中没有指定 IP 地址，则删除已经配置的所有 IP 和 MAC 的静态绑定表项。

【举例】

配置 IP 和 MAC 的静态绑定表项。

```
<Sysname> system-view
[Sysname] arp detection static-bind 192.168.1.2 2-1-201
```

1.5.4 arp detection trust

【命令】

arp detection trust

undo arp detection trust

【视图】

二层以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp detection trust 命令用来配置端口为 ARP 信任端口。**undo arp detection trust** 命令用来配置端口为 ARP 非信任端口。

缺省情况下，端口为 ARP 非信任端口。

【举例】

配置二层以太网接口 GigabitEthernet0/1 为 ARP 信任端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet0/1
[Sysname- GigabitEthernet0/1] arp detection trust
```

1.5.5 arp detection validate

【命令】

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dst-mac：检查 ARP 应答报文中的目的 MAC 地址，是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，无效的报文需要被丢弃。

ip：检查 ARP 报文源 IP 和目的 IP 地址，全 0、全 1、或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

src-mac：检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致认为有效，否则丢弃。

【描述】

arp detection validate 命令用来使能对 ARP 报文的目的或源 MAC 地址、IP 地址的有效性检查。使能有效性检查时可以指定某一种检查方式也可以配置成多种检查方式的组合。**undo arp detection validate** 命令用来关闭对 ARP 报文的有效性检查。关闭时可以指定关闭某一种或多种检查，在不指定检查方式时，表示关闭所有有效性检查。

缺省情况不对 ARP 报文的有效性检查。

需要注意的是，如果 **undo** 命令中没有指定检查方式，则关闭已经配置的所有检查方式。

【举例】

使能对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac src-mac ip
```

1.5.6 arp restricted-forwarding enable

【命令】

arp restricted-forwarding enable

undo arp restricted-forwarding enable

【视图】

VLAN 视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp restricted-forwarding enable 命令用来使能 ARP 报文强制转发功能。**undo arp restricted-forwarding enable** 命令用来关闭 ARP 报文强制转发功能。

缺省情况下，ARP 报文强制转发功能处于关闭状态。

【举例】

使能 VLAN 1 的 ARP 报文强制转发功能。

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp restricted-forwarding enable
```

1.5.7 display arp detection

【命令】

display arp detection

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

无

【描述】

display arp detection 命令用来显示使能了 ARP Detection 功能的 VLAN。

相关配置可参考 **arp detection enable**。

【举例】

显示所有使能了 ARP Detection 功能的 VLAN。

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1, 2, 4-5
```

表1-2 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	使能了ARP Detection功能的VLAN

1.5.8 display arp detection statistics

【命令】

display arp detection statistics [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface *interface-type interface-number*：显示指定接口的统计信息。*interface-type interface-number* 用来指定接口类型和编号。

【描述】

display arp detection statistics 命令用来显示 ARP Detection 功能报文检查的丢弃计数的统计信息。按端口显示用户合法性检查，报文有效性检查和 ARP 报文上送限速的统计情况，只显示丢弃的情况。不指定端口时，显示所有端口的统计信息。

【举例】

显示 ARP Detection 功能报文检查的丢弃计数的统计信息。

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP         Src-MAC    Dst-MAC    Inspect
GE0/1(U)                  40         0          0          78
GE0/2(U)                  0          0          0          0
GE0/3(T)                  0          0          0          0
GE0/4(U)                  0          0          30         0
```

表1-3 display arp detection statistics 命令显示信息描述表

字段	描述
Interface(State)	ARP报文入接口，State表示该接口的信任状态
IP	ARP报文源和目的IP地址检查不通过丢弃的报文计数
Src-MAC	ARP报文源MAC地址检查不通过丢弃的报文计数
Dst-MAC	ARP报文目的MAC地址检查不通过丢弃的报文计数
Inspect	ARP报文结合用户合法性检查（DHCP Snooping、802.1X、静态绑定）不通过丢弃的报文计数

1.5.9 reset arp detection statistics

【命令】

reset arp detection statistics [**interface** *interface-type interface-number*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

interface *interface-type interface-number*：表示清除指定接口下的统计信息。*interface-type interface-number* 用来指定接口类型和编号。

【描述】

reset arp detection statistics 命令用来清除 ARP Detection 的统计信息。不指定接口时，清除所有的 ARP Detection 统计信息。

【举例】

清除所有的 ARP Detection 统计信息。

```
<Sysname> reset arp detection statistics
```

1.6 ARP自动扫描、固化配置命令

1.6.1 arp fixup

【命令】

arp fixup

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp fixup 命令用来配置 Fixed ARP 功能。Fixed ARP 功能用来固化动态 ARP 表项，将动态 ARP 表项转换为静态 ARP 表项，用于指导报文转发。

需要注意的是：

- 固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。
- 固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。
- 如果用户执行固化前有 D 个动态 ARP 表项，S 个静态 ARP 表项，由于固化过程中存在动态 ARP 表项的老化或者新建动态 ARP 表项的情况，所以固化后的静态 ARP 表项可能为（D＋S＋M－N）个。其中，M 为固化过程中新建的动态 ARP 表项个数，N 为固化过程中老化的动态 ARP 表项个数。
- 通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* [*vpn-instance-name*] 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

【举例】

配置 Fixed ARP 功能。

```
<Sysname> system-view
[Sysname] arp fixup
```

1.6.2 arp scan

【命令】

arp scan [*start-ip-address* **to** *end-ip-address*]

【视图】

三层以太网接口视图/三层以太网子接口视图/VLAN 接口视图

【缺省级别】

2：系统级

【参数】

start-ip-address：ARP 扫描区间的起始 IP 地址。起始 IP 地址必须小于等于终止 IP 地址。

end-ip-address：ARP 扫描区间的终止 IP 地址。终止 IP 地址必须大于等于起始 IP 地址。

【描述】

arp scan 命令用来启动 ARP 自动扫描功能。

需要注意的是：

- 如果用户指定了 ARP 扫描区间，则对该范围内的邻居进行扫描；如果用户不指定 ARP 扫描区间，则对接口下的主 IP 地址网段内的邻居进行扫描。
- ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址（主 IP 地址或手工配置的从 IP 地址）在同一网段。
- 对于已存在 ARP 表项的 IP 地址不进行扫描。
- 扫描操作可能比较耗时，用户可以通过 Ctrl_C 来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

【举例】

对接口 GigabitEthernet0/1 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 0/1
[Sysname-GigabitEthernet0/1] arp scan
```

对接口 GigabitEthernet0/1 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 0/1
[Sysname-GigabitEthernet0/1] arp scan 1.1.1.1 to 1.1.1.20
```

目 录

1 Web过滤 ····· 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 ····· 1-7
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 ····· 1-9
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 ····· 1-11
1.1.13 firewall http url-filter host enable ····· 1-12
1.1.14 firewall http url-filter host ip-address ····· 1-12
1.1.15 firewall http url-filter host url-address ····· 1-13
1.1.16 firewall http url-filter parameter ····· 1-14
1.1.17 firewall http url-filter parameter enable ····· 1-15
1.1.18 reset firewall http ····· 1-16

1 Web过滤

说明

本手册所涉及的文件名遵循以下规则：

- “路径+文件名”的格式，即全文件名，则表示指定路径下的文件。全文件名长度为 1～135 个字符，不区分大小写，不包括结束符；
- “文件名”的格式，即只有文件名而没有路径，则表示当前工作路径下的文件。文件名的长度为 1～91 个字符，不区分大小写，不包括结束符。
- 不支持中文文件名。

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**]

【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，必须以“.”开头，为 1～9 个字符的字符串（包括“.”在内）。

verbose：显示 ActiveX 阻断的详细信息。

【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	匹配的次数
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**]

【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，必须以“.”开头，为 1～9 个字符的字符串（包括“.”在内）。

verbose：显示 Java Applet 阻断的详细信息。

【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

字段	描述
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**]

【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。

【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.
```

以上显示信息表示包含“^webfilter$”过滤关键字的 HTTP 请求报文已经匹配了 10 次。

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

字段	描述
Match-Times	匹配的次数
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.
 URL-filter host has loaded file “cfa0:/urlfilter”.
 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
URL-filter host has loaded file “cfa0:/urlfilter”	装载了网站地址过滤文件
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**]

【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。

【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              qqqqq
```

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	匹配的次数
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.
 URL-filter parameter has loaded file “cfa0:/parameterfilter”.
 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

字段	描述
URL-filter parameter has loaded file “cfa0:/parameterfilter”	装载了URL过滤参数文件
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，必须以“.”开头，为 1～9 个字符的字符串（包括“.”在内），不区分大小写，仅且只能包括一个“.”。

【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，必须以“.”开头，为 1～9 个字符的字符串（包括“.”在内），不区分大小写，只能由“0～9”、“a～z”、“A～Z”的有限组合构成。

【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】

permit：允许目标 URL 为 IP 地址的 Web 请求通过。

deny：拒绝目标 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】

permit：表示过滤行为为允许。

deny：表示过滤行为为拒绝。

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“0～9”、“a～z”、“A～Z、“.”、“-”、“_”、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

通配符	含义	使用说明
&	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“$”，表示精确匹配。例如，“^webfilter”表示以“webfilter”开头的网址（如 webfilter.com.cn）或类似于 cmm.webfilter-any.com 的网址将被过滤掉。关键字“^webfilter$”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

【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。
- 缺省过滤参数不允许使用命令 **firewall http url-filter parameter keywords** 和相应的 **undo** 命令添加或删除。

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 host 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
```