H3C SecPath 防火墙产品

DPI 深度安全命令参考(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W203-20191125
产品版本：

F100-C-EI/F100-C-G2/F100-S-G2/F100-M-G2/F100-C60-WiNet/F100-C80-WiNet/F1000-C8150/F1000-C8130/F1000-C8120/F100-C-A3/F100-C-A5/F100-C-A6	R9514
F100-A-G2/F100-A-EI/F100-E-G2/F100-E-EI/F100-A-SI/F1000-C-EI/F1000-C-G2/F1000-S-G2/F1000-A-G2/F1000-E-G2/F1000-C8180/F1000-C8170/F1000-C8160	R9323

前 言

本命令参考介绍了防火墙产品各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《DPI 深度安全命令参考》主要介绍 DPI 深度安全概述、应用层检测引擎、IPS、URL 过滤、数据过滤、文件过滤和防病毒相关的命令。

前言部分包含如下内容：

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

格　式	意　义
	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。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	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防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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。

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 应用层检测引擎

1.1 应用层检测引擎配置命令

1.1.1 app-profile

app-profile 命令用来创建DPI应用profile，并进入DPI应用profile视图。如果指定的DPI应用profile已经存在，则直接进入 DPI 应用 profile 视图。

undo app-profile 命令用来删除指定的 DPI 应用 profile。

【命令】

app-profile *profile-name*

undo app-profile *profile-name*

【缺省情况】

不存在 DPI 应用 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name：表示 DPI 应用 profile 的名称，为 1～63 个字符的字符串，不区分大小写，且只能为字母、数字、下划线。

【使用指导】

DPI（Deep Packet Inspection，深度报文检测）应用 profile 是一个安全业务模板，通过在 DPI 应用 profile 中引用 DPI 各业务策略（例如 IPS 策略、防病毒策略），并将其应用于对象策略规则或安全策略规则中来实现报文的应用层检测功能。

【举例】

创建一个名称为 abc 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc]
```

1.1.2 authentication enable

authentication enable 命令用来开启发送邮件的认证功能。

undo authentication enable 命令用来关闭发送邮件的认证功能。

【命令】

authentication enable

undo authentication enable

【缺省情况】

发送邮件的认证功能处于开启状态。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当通过命令 **email-server** 指定的邮件服务器需要认证时，可以开启发送邮件的认证功能，否则不需要开启此功能。

【举例】

关闭发送邮件的认证功能。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] undo authentication enable
```

1.1.3 block-period

block-period 命令用来配置报文源 IP 地址被阻断的时长。

undo block-period 命令用来恢复缺省情况。

【命令】

block-period *period*

undo block-period

【缺省情况】

报文源 IP 被阻断的时长为 1800 秒。

【视图】

应用层检测引擎的源阻断动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

period：报文源 IP 地址被阻断的时长，取值范围为 1～86400，单位为秒。

【使用指导】

如果设备上同时开启了黑名单功能，则报文的源 IP 地址被添加到 IP 黑名单后的老化时间为源阻断动作参数 profile 中配置的阻断时长。报文的源 IP 地址被加入 IP 黑名单后，阻断时长之内，后续来自该源 IP 地址的报文将被丢弃。

如果设备上未开启黑名单功能，报文会被阻断，且报文的源 IP 地址会被添加到 IP 黑名单，但 IP 黑名单功能并未生效。实现 IP 黑名单功能需要执行 **blacklist enable** 或 **blacklist global enable** 命令，有关此命令的详细介绍请参见“安全命令参考”中的“攻击检测与防范”。

【举例】

在名称为 b1 的应用层检测引擎源阻断动作参数 profile 中，配置报文源 IP 地址被阻断的时长为 3600 秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-para-b1] block-period 3600
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **inspect block-source parameter-profile**

1.1.4 capture-limit

capture-limit 命令用来配置捕获报文的最大字节数。

undo capture-limit 命令用来恢复缺省情况。

【命令】

capture-limit *kilobytes*

undo capture-limit

【缺省情况】

捕获报文的最大字节数为 512 千字节。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

kilobytes：表示捕获报文的最大字节数，取值范围为 0～1024，单位为千字节。

【使用指导】

捕获到的报文将被缓存到设备本地，当缓存的报文字节数达到指定上限值时，系统会将缓存的报文上传到指定的 URL 上，并清空本地缓存，然后重新开始捕获报文。如果配置捕获报文的最大字节数为 0，则系统会将捕获到的报文立刻上传到指定的 URL 上。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置捕获报文的最大值为 1024 千字节。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] capture-limit 1024
```

【相关命令】

- **inspect capture parameter-profile**
- **export url**
- **export repeating-at**

1.1.5 display inspect status

display inspect status 命令用来显示应用层检测引擎的工作状态。

【命令】

display inspect status

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示应用层检测引擎的运行状态。

```
<Sysname> display inspect status
Chassis 0 Slot 1:
 Running status: normal
```

表1-1 display inspect status 命令显示信息描述表

字段	描述
Running status	应用层检测引擎的运行状态，包括如下取值： • bypass by configure：因为配置原因引擎无法处理报文 • bypass by cpu busy：因为 CPU 使用率过高导致引擎无法处理报文 • normal：引擎工作正常

1.1.6 dns-server

dns-server 命令用来配置域名解析服务器的 IPv4 地址。

undo dns-server 命令用来恢复缺省情况。

【命令】

dns-server *ip-address*

undo dns-server

【缺省情况】

不存在域名解析服务器的 IPv4 地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address：表示域名服务器的 IPv4 地址，为点分十进制格式。

【使用指导】

如果配置的邮件服务器的地址为主机名格式，当设备发送日志信息邮件时，需要通过域名解析服务器获取邮件服务器 IP 地址与主机名的映射关系。

【举例】

配置域名解析的服务器地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] dns-server 192.168.0.1
```

1.1.7 email-server

email-server 命令用来配置邮件服务器的地址。

undo email-server 命令用来恢复缺省情况。

【命令】

email-server *address-string*

undo email-server

【缺省情况】

不存在邮件服务器的地址。

【视图】

应用层检测引擎的邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string：表示邮件服务器的地址，为 3～63 个字符的字符串，区分大小写。

【使用指导】

配置的邮件服务器地址的地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

说明

采用主机名时，需要确保设备能通过静态或动态域名解析方式获得邮件服务器的 IP 地址，并与之路由可达。否则邮件发送会失败。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”

【举例】

配置邮件服务器地址为 rndcas.123.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server rndcas.123.com
```

配置邮件服务器地址为 192.168.1.1。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server 192.168.1.1
```

1.1.8 export repeating-at

export repeating-at 命令用来配置每天定时上传捕获报文的时间。

undo export repeating-at 命令用来恢复缺省情况。

【命令】

export repeating-at *time*

undo export repeating-at

【缺省情况】

每天凌晨 1 点定时上传捕获报文。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

time：表示每天上传捕获报文的时间，格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

【使用指导】

每天指定的时间到达时，无论本地缓存是否达到最大值，系统将向指定的 URL 上传缓存的捕获报文，并清空本地缓存。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置每天定时上传捕获报文的时间为凌晨 2 点。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] export repeating-at 02:00:00
```

【相关命令】

- **inspect capture parameter-profile**
- **export url**
- **capture-limit**

1.1.9 export url

export url 命令用来配置上传捕获报文的 URL。

undo export url 命令用来恢复缺省情况。

【命令】

export url *url-string*

undo export url

【缺省情况】

未指定上传捕获报文的 URL。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：表示用于上传捕获报文的 URL，为 1～255 个字符的字符串。

【使用指导】

本地缓存的捕获的报文字节数达到指定上限值或者每天指定的时间到达时，系统会将缓存的报文上传到指定的 URL。如果未配置上传捕获报文的 URL，则系统依然会上传捕获到的报文，但是会上传失败。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置上传捕获报文的 URL 为 tftp://192.168.100.100/upload。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-c1] export url tftp://192.168.100.100/upload
```

【相关命令】

- **inspect capture parameter-profile**

- **capture-limit**
- **export repeating-at**

1.1.10 inspect activate

inspect activate 命令用来激活 DPI 各业务模块的策略和规则配置。

【命令】

inspect activate

【缺省情况】

DPI 各业务模块的策略和规则被创建、修改和删除时不生效。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当 DPI 各业务模块（比如 IPS 和防病毒等特性）的策略和规则被创建、修改和删除后，需要执行 **inspect activate** 命令来使其策略和规则配置生效。

当 DPI 各业务模块的策略和规则被创建、修改和删除且保存配置的情况下，设备重启之后，其相关的所有策略和规则配置也会生效。

执行此命令会暂时中断 DPI 业务的处理，为了避免重复执行此命令对 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执行此命令。

【举例】

激活 DPI 各业务模块的策略和规则配置。

```
<Sysname> system-view
[Sysname] inspect activate
```

1.1.11 inspect block-source parameter-profile

inspect block-source parameter-profile 命令用来创建应用层检测引擎的源阻断动作参数 profile，并进入源阻断动作参数 profile 视图。如果指定的源阻断动作参数 profile 已经存在，则直接进入源阻断动作参数 profile 视图。

undo inspect block-source parameter-profile 命令删除应用层检测引擎的源阻断动作参数 profile。

【命令】

inspect block-source parameter-profile *parameter-name*

undo inspect block-source parameter-profile *parameter-name*

【缺省情况】

不存在源阻断动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name：源阻断动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入源阻断动作参数 profile 视图后，可以配置对报文执行源阻断动作时采用的特定参数，比如阻断时长。

【举例】

创建名称为 b1 的应用层检测引擎源阻断动作参数 profile，并进入源阻断动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-para-b1]
```

【相关命令】

- **block-period**

1.1.12 inspect bypass

inspect bypass 命令用来关闭应用层检测引擎功能。

undo inspect bypass 命令用来开启应层检测引擎功能。

【命令】

inspect bypass

undo inspect bypass

【缺省情况】

应用层检测引擎功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

应用层检测引擎对报文的检测是一个复杂且会占用一定的系统资源的过程。开启应用层检测功能后，如果出现 CPU 使用率过高等情况时，可以通过关闭此功能来保证设备的正常运行。

关闭应层检测引擎功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。

【举例】

关闭应用层检测引擎功能。

```
<Sysname> system-view
[Sysname] inspect bypass
```

【相关命令】

- **display inspect status**

1.1.13 inspect cache-option maximum

inspect cache-option maximum 命令用来配置应用层检测引擎缓存待检测规则的选项的最大数目。

undo cache-option 命令用来恢复缺省情况。

【命令】

inspect cache-option maximum *max-number*

undo inspect cache-option

【缺省情况】

应用层检测引擎缓存待检测规则的选项的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number：指定应用层检测引擎在检测报文时，对每条 TCP/UDP 流缓存待检测规则的选项的最大数目，取值范围为 1～254。

【使用指导】

应用层检测引擎中的检测规则是由各个 DPI 业务模块中的规则或特征转换而成。

有时应用层检测引擎在检测一条 TCP/UDP 数据流时，虽然匹配上了一个或多个关键字，但是只根据当前 TCP/UDP 报文的内容，不能确定检测规则是否能够被匹配上，因此需要对这些检测规则的选项进行缓存，通过继续检测后续报文是否能够匹配上这些检测规则的选项，来判断是否能识别出此条 TCP/UDP 数据流的应用或行为。

通常，使用缺省配置即可满足应用需求。但是在某些场景中，为了提高应用层检测引擎对 TCP/UDP 数据流应用或行为的识别能力和准确率，需要将应用层检测引擎当前缓存待检测选项的最大数调高，调高后，每条数据流占用的内存可能会上升。同理某些场景下，设备内存使用率偏高，可以调低这个参数，提高设备性能，以保证基础的数据转发正常进行。

例如当前应用层检测引擎有 5000 条检测规则，每条检测规则有一个关键字，那么当前应用层检测引擎中一共有 5000 个关键字。应用层检测引擎需要检测一条 TCP/UDP 数据流的报文的载荷部分是否存在这 5000 个关键字，一种可能的情况是当前报文中存在 10 个关键字。根据应用层检测引擎的工作原理可知，这 10 个关键字所属的 10 条检测规则，要求关键字之后的载荷部分各自需要匹配

出 10 个不同的选项，因为每个选项都是对一个完整 TCP/UDP 数据流的检测，所以仅仅根据当前报文载荷就不能确定这些选项是否能被匹配上。因此需要针对这条 TCP/UDP 数据流缓存 10 个选项，通过继续检测后续报文是否能够匹配上这些检测规则的选项，来判断是否能识别出此条 TCP/UDP 数据流的应用层或行为。

一般一个检测规则可以对应多个关键字，每个关键字对应多个选项。

【举例】

配置应用层检测引擎缓存待检测规则的选项的最大数目为 4。

```
<Sysname> system-view
[Sysname] inspect cache-option maximum 4
```

1.1.14 inspect capture parameter-profile

inspect capture parameter-profile 命令用来创建应用层检测引擎的捕获动作参数 profile，并进入捕获动作参数 profile 视图。如果指定的捕获动作参数 profile 已经存在，则直接进入捕获动作参数 profile 视图。

undo inspect capture parameter-profile 命令用来删除应用层检测引擎的捕获动作参数 profile。

【命令】

inspect capture parameter-profile *parameter-name*

undo inspect capture parameter-profile *parameter-name*

【缺省情况】

不存在捕获动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name：捕获动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入捕获动作参数 profile 视图后，可以配置执行报文捕获动作时采用的特定参数，比如本地缓存报文的最大值字节数。

【举例】

创建名称为 c1 的应用层检测引擎捕获动作参数 profile，并进入捕获动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-para-b1]
```

【相关命令】

- **capture-limit**
- **export repeating-at**

- **export url**

1.1.15 inspect cpu-threshold disable

inspect cpu-threshold disable 命令用来关闭 CPU 门限响应功能。

undo inspect cpu-threshold disable 命令用来恢复 CPU 门限响应功能。

【命令】

inspect cpu-threshold disable

undo inspect cpu-threshold disable

【缺省情况】

CPU 门限响应功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

应用层检测引擎对报文的检测是一个比较复杂且会占用一定系统资源的过程。当设备的 CPU 利用率较高时，应用层检测引擎 CPU 门限响应功能会启动如下机制来缓解系统资源紧张的问题。

- 当 CPU 利用率达到设备上配置的 CPU 利用率阈值时，系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。
- 当设备的 CPU 利用率恢复到或低于设备上配置的 CPU 利用率恢复阈值时，系统会恢复应用层检测引擎的检测功能。

在系统 CPU 占用率较高的情况下，不建议用户关闭此功能。

【举例】

关闭 CPU 门限响应功能。

```
<Sysname> system-view
[Sysname] inspect cpu-threshold disable
```

【相关命令】

- **display inspect status**
- **inspect bypass**
- **inspect stream-fixed-length disable**

1.1.16 inspect email parameter-profile

inspect email parameter-profile 命令用来创建应用层检测引擎的邮件动作参数 profile，并进入邮件动作参数 profile 视图。如果指定的邮件动作参数 profile 已经存在，则直接进入邮件动作参数 profile 视图。

undo inspect email parameter-profile 命令删除应用层检测引擎邮件动作参数 profile。

【命令】

inspect email parameter-profile *parameter-name*

undo inspect email parameter-profile *parameter-name*

【缺省情况】

不存在邮件动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name：邮件动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入邮件动作参数 profile 视图后，可以配置执行发送邮件动作时采用的特定参数，比如邮件服务器的地址、发件人与收件人的地址和登录邮件服务器的用户名和密码等信息。

【举例】

创建名称为 c1 的应用层检测引擎邮件动作参数 profile，并进入邮件动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1]
```

1.1.17 inspect logging parameter-profile

inspect logging parameter-profile 命令用来创建应用层检测引擎的日志动作参数 profile，并进入日志动作参数 profile 视图。如果指定的日志动作参数 profile 已经存在，则直接进入日志动作参数 profile 视图。

undo inspect logging parameter-profile 命令用来删除应用层检测引擎的日志动作参数 profile。

【命令】

inspect logging parameter-profile *parameter-name*

undo inspect logging parameter-profile *parameter-name*

【缺省情况】

不存在日志动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name：日志动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入日志动作的参数 profile 视图后，可以配置生成报文日志时采用的特定参数，比如输出日志的方式。

【举例】

创建名称为 log1 的应用层检测引擎的日志动作参数 profile，并进入日志动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-logging-para-log1]
```

【相关命令】

- **log**

1.1.18 inspect optimization disable

inspect optimization disable 命令用来关闭指定的应用层检测引擎的优化调试功能。

undo inspect optimization disable 命令用来开启指定的应用层检测引擎的优化调试功能。

【命令】

inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

undo inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

【缺省情况】

应用层检测引擎的所有优化调试功能均处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

chunk：表示应用层检测引擎对 Chunk 格式报文进行解码的优化调试功能。

no-acsignature：表示应用层检测引擎对没有关键字检测规则进行检测的优化调试功能。

raw：表示应用层检测引擎对未经解码 TCP/UDP 的应用层载荷字段进行检测的优化调试功能。

uncompress：表示应用层检测引擎对 HTTP Body 字段进行解压缩的优化调试功能。

url-normalization：表示应用层检测引擎对 HTTP URL 字段进行正规化校准的优化调试功能。

【使用指导】

如果不指定任何参数，则表示关闭或开启应用层检测引擎的所有优化调试功能。

有关应用层检测引擎的各种优化调试功能的详细介绍如下：

应用层检测引擎对 Chunk 格式报文进行解码的优化调试功能：Chunk 是 HTTP 协议载荷(Body)的一种传输方式，对于以 Chunk 方式传输的 HTTP 协议的载荷，需要先对其进行解码以获取真正的载荷内容。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来关闭应层检测引擎解码 Chunk 格式报文的功能，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

应用层检测引擎对没有关键字检测规则进行检测的优化调试功能：没有关键字的检测规则是指此规则不是基于字符串匹配进行检测，而是基于报文的端口号、错误码等字段进行检测。缺省情况下应用层检测引擎对没有关键字的检测规则进行检测，但是在某些场景下，如果设备的吞吐量较差，不能满足客户基本的通信需求，此时可以配置应用层检测引擎对没有关键字的检测规则不进行检测，以提高设备的性能，保证用户最基础的网络通信。

应用层检测引擎对未经解码 TCP/UDP 的应用层载荷字段进行检测的优化调试功能：有些 TCP/UDP 数据流的应用层协议（例如 HTTP、SMTP、POP3、IMAP4）涉及编码和解码处理，而对该类数据流的应用层内容的检测需要在对报文载荷进行解码之后进行。如果当前设备的处理性能不能满足用户基本的通信需求，可以通过该命令取消对未解码的应用层载荷字段的检测，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对报文载荷内容的应用或行为的识别能力会受到影响。

应用层检测引擎对 HTTP Body 字段进行解压缩的优化调试功能：如果报文的 HTTP Body 字段是压缩编码，应用层检测引擎需要先对 HTTP Body 字段进行解压缩后，才能对此字段的内容进行检测。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来取消对 HTTP Body 字段的压缩编码进行解压缩处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

应用层检测引擎对 HTTP URL 字段进行正规化校准的优化调试功能：对 HTTP URL 字段进行正规化校准功能是指把 URL 中绝对路径字调整为常规路径格式，对特殊的路径字段进行调整和正确性检查。例如报文 URL 中绝对路径部分输入的是 test/dpi/../index.html，正规化处理后是 test/index.html。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来取消对 HTTP URL 字段进行正规化校准处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

【举例】

关闭应用层检测引擎的所有优化调试功能。

```
<Sysname> system-view
[Sysname] inspect optimization disable
```

1.1.19 inspect packet maximum

inspect packet maximum 命令用来配置应用层检测引擎可检测有载荷内容的报文的最大数目。

undo inspect packet 命令用来恢复缺省情况。

【命令】

inspect packet maximum *max-number*

undo inspect packet

【缺省情况】

应用层检测引擎可检测有载荷内容的报文的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number：指定应用层检测引擎检测有载荷内容的报文的最大数目，取值范围为 1～254。

【使用指导】

应用层检测引擎在对一个数据流的第一个有载荷内容的报文进行检测时，如果没有匹配上任何检测规则，则需要继续检测此数据流的第二个有载荷内容的报文，以此类推。如果直到设备设置的最大报文检测个数还未匹配上任何检测规则，则表示对此数据流匹配失败，并直接允许此数据流通过。

通常，使用缺省配置即可满足应用需求。但是在某些应用场景中，应用层检测引擎在检测有载荷内容的报文的个数达到指定的个数之后，仍然不能识别当前报文应用层信息的应用或行为，此时需要调高这个参数。调高此参数后，设备的吞吐量性能会下降，但是应用识别的成功率会增加。同理在设备吞吐量较差，不能满足客户需求的应用场景中，此时需要调低这个参数，调低参数后，吞吐量会增加，但是应用识别成功率会降低。

【举例】

配置应用层检测引擎可检测有载荷内容的报文的最大数目为 16。

```
<Sysname> system-view
[Sysname] inspect packet maximum 16
```

1.1.20 inspect redirect parameter-profile

inspect redirect parameter-profile 命令用来创建应用层检测引擎的重定向动作参数 profile，并进入重定向动作参数 profile 视图。如果指定的重定向动作参数 profile 已经存在，则直接进入重定向动作参数 profile 视图。

undo inspect redirect parameter-profile 命令删除应层检测引擎的重定向动作参数 profile。

【命令】

inspect redirect parameter-profile *parameter-name*

undo inspect redirect parameter-profile *parameter-name*

【缺省情况】

不存在重定向动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name：重定向动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

进入重定向动作参数 profile 视图后，可以配置对报文执行重定向动作时采用的特定参数，比如对报文重定向的 URL。

【举例】

创建名称为 r1 的应用层检测引擎重定向动作参数 profile，并进入重定向动作参数 profile 视图。

```
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1]
```

1.1.21 inspect signature auto-update proxy

inspect signature auto-update proxy 命令用来配置 DPI 业务特征库在线升级所使用的代理服务器。

undo inspect signature auto-update proxy 命令用来恢复缺省情况。

【命令】

inspect signature auto-update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* **password** { **cipher** | **simple** } *string*]

undo inspect signature auto-update proxy

【缺省情况】

未配置 DPI 业务特征库在线升级所使用的代理服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定代理服务器的域名。*domain-name* 表示代理服务器的域名，为 3～63 个字符的字符串，不区分大小写。

ip *ip-address*：指定代理服务器的 IP 地址，仅支持 IPv4 类型地址。

port *port-number*：指定代理服务器的端口号，取值范围为 1～65535，缺省值为 80。

user *user-name*：指定登录代理服务器的用户名。*user-name* 表示用户名，为 1～31 个字符的字符串，不区分大小写。

password：指定登录代理服务器的用户密码。

cipher：表示以密文方式设置密码。

simple：表示以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～31 个字符的字符串，密文密码为 1～73 个字符的字符串。

【使用指导】

当 DPI 业务模块（例如 IPS 和 URL 过滤）的特征库进行在线升级时，若设备不能连接到 H3C 官方网站，则可配置一个代理服务器使设备连接到 H3C 官方网站上的特征库服务专区，进行特性库在线升级。有关特征库在线升级功能的详细介绍，请参见各 DPI 业务配置指导手册中的“特征库升级与回滚”。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DPI 业务特征库在线升级所使用的代理服务器域名为 www.abc.com，端口号为 8888，登录代理服务器的用户名和密码均为 admin。

```
<Sysname> system-view
[Sysname] inspect signature auto-update proxy domain www.abc.com port 8888 user admin
password simple admin
```

1.1.22 inspect stream-fixed-length disable

inspect stream-fixed-length disable 命令用来关闭应用层检测引擎检测固定长度数据流功能。

undo inspect stream-fixed-length disable 命令用来开启应用层检测引擎检测固定长度数据流功能。

【命令】

inspect stream-fixed-length disable

undo inspect stream-fixed-length disable

【缺省情况】

应用层检测引擎检测固定长度数据流功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

应用层检测引擎检测固定长度数据流功能，是指应用层检测引擎只检测每条数据流首包后固定长度内的数据，不再检测超出固定长度后的数据。

【举例】

关闭应用层检测引擎检测固定长度数据流功能。

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length disable
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length**

1.1.23 inspect stream-fixed-length

inspect stream-fixed-length 命令用来配置应用层检测引擎检测数据流的固定长度。

undo inspect stream-fixed-length 命令用来恢复缺省情况。

【命令】

inspect stream-fixed-length { **email** | **ftp** | **http** } * *length*

undo inspect stream-fixed-length

【缺省情况】

应用层检测引擎对 FTP 协议、HTTP 协议和与 E-mail 相关协议数据流的固定检测长度均为 32 千字节。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

email：表示设置检测与 E-mail 协议相关类型数据流的固定长度，支持的 E-mail 协议包括 SMTP、POP3 和 IMAP。

ftp：表示设置检测 FTP 协议类型数据流的固定长度。

http：表示设置检测 HTTP 协议类型数据流的固定长度。

length：表示设置检测指定协议类型数据流的固定长度，取值范围为 1～128，单位为千字节。

【使用指导】

调高此参数后，设备的吞吐量性能会下降，但是应用层信息识别的成功率会提高；同理调低参数后，设备的吞吐量会增加，但是应用层信息识别的成功率会降低。

【举例】

配置应用层检测引擎检测 FTP 协议类型数据流的固定长度为 35 千字节，检测 HTTP 协议类型数据流的固定长度为 40 千字节。

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length ftp 35 http 40
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length disable**

1.1.24 inspect tcp-reassemble enable

inspect tcp-reassemble enable 命令用来开启 TCP 数据段重组功能。

undo inspect tcp-reassemble enable 命令用来关闭 TCP 数据段重组功能。

【命令】

inspect tcp-reassemble enable

undo inspect tcp-reassemble enable

【缺省情况】

TCP 数据段重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

大量的 TCP 乱序数据段极有可能会造成应用层检测引擎对此 TCP 数据流检测失败。例如应用层检测引擎需要检测 TCP 载荷中是否包含关键字“this is a secret”，由于数据段乱序，可能含有“a secret”的数据段先到达设备，含有“this is”的数据段后到达设备，这样就会造成应用层检测引擎对此 TCP 数据流检测失败。

为了提高应用层检测引擎对 TCP 数据流检测的准确率，可以在设备上开启 TCP 数据段重组功能。当接收到乱序的 TCP 数据段时，设备会将此数据段和来自于同一条数据流的后续数据段暂时保存至缓冲区，进行 TCP 数据段重组，完成数据段重组再送往后续流程处理。

若缓冲区中已缓存的数据段数目达到最大值（可以通过 **inspect tcp-reassemble max-segment** 命令来配置）时仍无法成功重组，则设备直接将已缓存的乱序数据段和此条数据流的所有后续 TCP 数据段送往后续流程处理，不再进行 TCP 重组。这样可以降低对设备转发性能的影响。

【举例】

开启 TCP 数据段重组功能。

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble enable
```

【相关命令】

- **inspect tcp-reassemble max-segment**

1.1.25 inspect tcp-reassemble max-segment

inspect tcp-reassemble max-segment 命令用来配置 TCP 重组缓冲区可缓存的 TCP 数据段最大数目。

undo inspect tcp-reassemble max-segment 命令用来恢复缺省情况。

【命令】

inspect tcp-reassemble max-segment *max-number*

undo inspect tcp-reassemble max-segment

【缺省情况】

TCP 重组缓冲区可缓存的 TCP 数据段最大数目为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number：表示 TCP 重组缓冲区可缓存的 TCP 数据段最大数目，取值范围为 10～50。

【使用指导】

在存在大量 TCP 乱序数据段的网络环境中，调高此参数，则可提高应用层检测引擎对 TCP 数据段检测的准确率，但是设备转发性能可能会下降。若调低此参数可避免因长时间缓存 TCP 数据段而造成设备转发性能下降，但是应用层检测引擎对 TCP 数据段检测的准确率会降低。请根据实际情况调整此参数。

仅开启 TCP 数据段重组功能后，此命令才生效。

【举例】

配置 TCP 重组缓冲区中可缓存的 TCP 数据段最大数目为 20 个

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble max-segment 20
```

【相关命令】

- **inspect tcp-reassemble enable**

1.1.26 log

log 命令用来配置记录报文日志的方式。

undo log 命令用来取消指定的记录报文日志的方式。

【命令】

log { **email** | **syslog** }

undo log { **email** | **syslog** }

【缺省情况】

报文日志被输出到信息中心。

【视图】

应用层检测引擎的日志动作的参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

email：表示将日志以邮件的方式发送到指定的收件人邮箱。

syslog：表示将日志输出到信息中心。

【举例】

在名称为log1的应用层检测引擎日志动作参数profile中，配置将生成的报文日志输出到信息中心。

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-log-para-log1] log syslog
```

【相关命令】

- **inspect logging parameter-profile**

1.1.27 password

password 命令用来配置登录邮件服务器的密码。

undo password 命令用来恢复缺省情况。

【命令】

password { **cipher** | **simple** } *string*

undo password

【缺省情况】

不存在登录邮件服务器的密码。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

cipher：表示以密文方式设置用户密码。

simple：表示以明文方式设置用户密码，该密码将以密文形式存储。

string：表示登录邮件服务器的密码。明文密码为 1～63 个字符的字符串，密文密码为 1～117 个字符的字符串，区分大小写。

【使用指导】

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置登录邮件服务器的明文密码为 abc123。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] password simple abc123
```

【相关命令】

- **authentication enable**

1.1.28 receiver

receiver 命令用来配置收件人地址。

undo receiver 命令用来恢复缺省情况。

【命令】

receiver *address-string*

undo receiver

【缺省情况】

不存在收件人地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string：表示收件人地址，为 3～511 个字符的字符串，区分大小写。

【使用指导】

收件人地址可以同时输入多个，且每个收件人地址之间用英文“;”号隔开。

【举例】

配置收件人的地址为 123@abc.com 和 nnn@abc.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] receiver 123@abc.com;nnn@abc.com
```

1.1.29 redirect-url

redirect-url 命令用来配置重定向 URL。

undo redirect-url 命令用来恢复缺省情况。

【命令】

redirect-url *url-string*

undo redirect-url

【缺省情况】

不存在重定向 URL。

【视图】

应层检测引擎的重定向动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：表示重定向 URL，为 9～63 个字符的字符串，区分大小写。该 URL 必须以 http://或 https://开头，例如 http://www.baidu.com。

【使用指导】

当需要把匹配成功的报文重定向到某个 Web 界面时，可以通过执行此命令来指定重定向 URL。

【举例】

配置重定向 URL 为 http://www.abc.com/upload。

```
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1] redirect-url http://www.abc.com/upload
```

【相关命令】

- **inspect redirect parameter-profile**

1.1.30 secure-authentication enable

secure-authentication enable 命令用开启安全传输登录邮件服务器密码功能。

undo secure-authentication enable 命令用来关闭安全传输登录邮件服务器密码功能。

【命令】

secure-authentication enable

undo secure-authentication enable

【缺省情况】

安全传输登录邮件服务器密码功能处于关闭状态。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启此功能后，首先在设备与邮件服务器之间创建一条安全通道，然后再在此通道中传输登录邮件服务器的密码。

【举例】

开启安全传输登录邮件服务器密码功能。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] secure-authentication enable
```

【相关命令】

- **authentication enable**

1.1.31 sender

sender 命令用来配置发件人地址。

undo sender 命令用来恢复缺省情况。

【命令】

sender *address-string*

undo sender

【缺省情况】

不存在发件人地址。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string：表示发件人地址，为 3～63 个字符的字符串，区分大小写。

【使用指导】

发件人地址是指设备向目的地发送邮件时使用的源地址。

【举例】

配置发件人的地址为 abc@123.com。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] sender abc@123.com
```

1.1.32 username

username 命令用来配置登录邮件服务器的用户名。

undo username 命令用来恢复缺省情况。

【命令】

username *name-string*

undo username

【缺省情况】

不存在登录邮件服务器的用户名。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

name-string：表示登录邮件服务器的用户名。为 1～63 个字符的字符串，区分大小写。

【使用指定】

在同一个邮件动作参数 profile 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置登录邮件服务器的用户名为 han。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] username han
```

【相关命令】

- **authentication enable**

目 录

1 IPS

1.1 IPS配置命令

1.1.1 action

action 命令用来配置筛选 IPS 特征的动作属性。

undo action 命令用来恢复缺省情况。

【命令】

action { **block-source** | **drop** | **permit** | **reset** } *

undo action

【缺省情况】

IPS 策略匹配所有动作的特征。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source：表示源阻断动作，该动作阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单。

drop：表示丢弃报文的动作。

permit：表示允许报文通过的动作。

reset：表示重置动作，该动作通过发送 TCP 的 reset 报文使 TCP 连接断开。

【使用指导】

可通过配置动作属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个动作，只要符合其中一个，具有该动作属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中配置筛选 IPS 特征的动作为 drop 和 reset。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] action drop reset
```

1.1.2 attack-category

attack-category 命令用来配置筛选 IPS 特征的攻击分类属性。

undo attack-category 命令用来删除筛选 IPS 特征的攻击分类属性。

【命令】

attack-category { *category* [*subcategory*] | **all**}

undo attack-category { *category* [*subcategory* | **all**] }

【缺省情况】

IPS 策略匹配所有攻击分类的特征。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

category：表示设备中已有的攻击分类名称。

subcategory：表示设备中已有攻击分类中的子分类名称。若不指定本参数，则表示指定攻击分类中的所有子分类。

all：表示设备中已有的所有攻击分类。

【使用指导】

可通过配置攻击分类属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个攻击分类。只要符合其中一个，具有该攻击分类的特征将会被筛选出来。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的攻击分类为 Vulnerability 攻击分类中的 SQL-Injection 子分类。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] attack-category Vulnerability SQL-Injection
```

1.1.3 display ips policy

display ips policy 命令用来显示 IPS 策略信息。

【命令】

display ips policy *policy-name*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

policy-name：表示 IPS 策略名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

显示 IPS 策略 aa 的策略信息。

```
<Sysname> display ips policy aa
Total signatures        :474       failed:0
 Pre-defined  signatures:474       failed:0
 User-defined signatures:0         failed:0

Flag:
  B: Block-source  D: Drop  P: Permit  Rs: Reset  Rd: Redirect  C: Capture  L: L
ogging
  Pre: predefined  User: user-defined

Type RuleID    Target      SubTarget       Severity Category    Status  Action
Pre  1         OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  2         OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  3         Browser     Browser/Interne High     Vulnerabili Enable  RsCL
Pre  4         OfficeSoftw OfficeSoftware/ High     Vulnerabili Enable  RsL
Pre  5         OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  6         OperationSy OperationSystem High     Vulnerabili Disable PL
Pre  7         Browser     Browser/Interne High     Vulnerabili Disable PL
Pre  8         Application ApplicationSoft High     Vulnerabili Enable  RsL
Pre  9         Application ApplicationSoft High     Vulnerabili Enable  RsL
Pre  10        OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  11        Browser     Browser/Interne High     Vulnerabili Enable  RsL
Pre  12        OfficeSoftw OfficeSoftware/ Critical Vulnerabili Disable RsL
Pre  13        OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  14        Application ApplicationSoft High     Vulnerabili Enable  RsL
Pre  15        Browser     Browser/Interne High     Vulnerabili Enable  RsL
Pre  16        OperationSy OperationSystem Critical Vulnerabili Enable  RsL
Pre  17        Browser     Browser/Interne High     Vulnerabili Enable  RsL
Pre  18        OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  19        OfficeSoftw OfficeSoftware/ Critical Vulnerabili Disable RsL
Pre  20        OfficeSoftw OfficeSoftware/ Critical Vulnerabili Enable  RsL
Pre  21        Application ApplicationSoft Critical Vulnerabili Enable  RsL
Pre  23        OperationSy OperationSystem High     Vulnerabili Enable  RsL
Pre  24        Browser     Browser/Interne High     Vulnerabili Disable PL
Pre  25        NetworkDevi NetworkDevice/D High     Vulnerabili Enable  PL
Pre  26        Browser     Browser/Interne High     Vulnerabili Enable  RsL
---- More ----
```

表1-1 display ips policy 命令显示信息描述表

字段	描述
Total signatures	IPS特征总数
Pre-defined signatures	预定义IPS特征数目

字段	描述
User-defined signatures	用户自定义IPS特征数目
Type	IPS特征的类型，包括如下取值： • Pre：表示预定义特征 • User：表示自定义特征
RuleID	IPS特征编号
Target	攻击对象
SubTarget	攻击子对象
Severity	IPS特征的攻击严重程度属性，从低到高分为四级：Low、Medium、High、Critical
Category	IPS特征的攻击类别名称
Status	IPS特征的状态，包括如下取值： • Enabled：表示此特征已生效 • Disabled：表示此特征未生效
Action	对报文的处理动作，包括如下取值： • Block-source：表示阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单 • Drop：表示丢弃符合特征的报文 • Permit：表示允许符合特征的报文通过 • Reset：表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 • Redirect：表示重定向符合特征的报文 • Capture：表示捕获符合特征的报文 • Logging：表示对符合特征的报文生成日志

【相关命令】

- **ips policy**

1.1.4 display ips signature

display ips signature 命令用来显示 IPS 特征信息。

【命令】

display ips signature [**pre-defined** | **user-defined**] [**direction** { **any** | **to-client** | **to-server** }] [**category** *category-name* | **fidelity** { **high** | **low** | **medium** } | **protocol** { **icmp** | **ip** | **tcp** | **udp** } | **severity** { **critical** | **high** | **low** | **medium** }] *

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

pre-defined：显示预定义 IPS 特征。

user-defined：显示自定义 IPS 特征。

direction { **any** | **to-client** | **to-server** }：显示符合指定方向属性的 IPS 特征。如果未指定此参数，则显示所有方向上的 IPS 特征。

- **to-server**：表示一个会话的客户端到服务器的方向。
- **to-client**：表示一个会话的服务器到客户端的方向。
- **any**：表示一个会话的两个方向。

category *category-name*：显示符合指定攻击类别属性的 IPS 特征，*category-name* 是攻击类型的名称。如果未指定此参数，则显示所有攻击类型的 IPS 特征。

fidelity { **high** | **low** | **medium** }：显示符合指定可信度属性的 IPS 特征。如果未指定此参数，则显示所有可信度的 IPS 特征。可信度是指此 IPS 特征识别攻击行为准确度，且从低到高分为如下三个级别：

- **low**：可信度比较低。
- **medium**：可信度中等。
- **high**：可信度比较高。

protocol { **icmp** | **ip** | **tcp** | **udp** }：显示符合指定协议属性的 IPS 特征，协议 ICMP、IP、TCP 和 UDP 协议。如果未指定此参数，则显示所有协议的 IPS 特征。

severity { **critical** | **high** | **low** | **medium** }：显示符合指定攻击严重程度属性的 IPS 特征。如果未指定此参数，则显示所有攻击严重程度的 IPS 特征。攻击严重程度是指匹配此 IPS 特征的网络攻击造成的危害的严重程度，且从低到高分为四个级别：

- **low**：攻击严重程度比较低。
- **medium**：攻击严重程度中等。
- **high**：攻击严重程度比较高。
- **critical**：攻击严重程度非常高。

【使用指导】

若不指定任何参数，则显示所有 IPS 特征。

【举例】

显示可信度为中等的所有 TCP 协议的预定义 IPS 特征。

```
<Sysname> display ips signature pre-defined protocol tcp fidelity medium
Pre-defined  signatures:465       failed:0

Flag:
  Pre: predefined   User: user-defined

Type Sig-ID    Direction Severity Fidelity Category      Protocol
Pre  1         To-server High     Medium   Vulnerability TCP
```

```
Pre  2         To-server High     Medium   Vulnerability TCP
Pre  3         To-client High     Medium   Vulnerability TCP
Pre  4         To-client High     Medium   Vulnerability TCP
Pre  5         To-client High     Medium   Vulnerability TCP
Pre  6         To-client High     Medium   Vulnerability TCP
Pre  7         To-client High     Medium   Vulnerability TCP
Pre  8         To-client High     Medium   Vulnerability TCP
Pre  10        To-server High     Medium   Vulnerability TCP
Pre  11        To-client High     Medium   Vulnerability TCP
Pre  12        To-client Critical Medium   Vulnerability TCP
Pre  13        To-client High     Medium   Vulnerability TCP
Pre  14        To-server High     Medium   Vulnerability TCP
Pre  15        To-client High     Medium   Vulnerability TCP
Pre  16        To-client Critical Medium   Vulnerability TCP
Pre  17        To-client High     Medium   Vulnerability TCP
Pre  18        To-client High     Medium   Vulnerability TCP
---- More ----
```

显示攻击严重程度为比较高的所有 UDP 协议的 IPS 特征。

```
<Sysname> display ips signature severity high protocol udp
Total signatures        :7         failed:0
 Pre-defined  signatures:7         failed:0
 User-defined signatures:0         failed:0

Flag:
  Pre: predefined   User: user-defined

Type Sig-ID    Direction Severity Fidelity Category      Protocol
Pre  9         To-server High     Medium   Vulnerability UDP
Pre  45        To-server High     Medium   Vulnerability UDP
Pre  187       Any       High     Medium   Vulnerability UDP
Pre  196       Any       High     Medium   Vulnerability UDP
Pre  223       To-server High     Medium   Vulnerability UDP
Pre  234       To-client High     Medium   Vulnerability UDP
Pre  338       To-client High     Medium   Vulnerability UDP
```

表1-2 display ips signature 命令显示信息描述表

字段	描述
Total signatures	IPS特征总数
failed	Snort规则导入特征库失败和特征库加载失败的特征总数
Pre-defined count	预定义IPS特征数目
User-defined count	自定义IPS特征数目
Type	IPS特征的类型，包括如下取值： • Pre：表示预定义特征 • User：表示自定义特征
Sig-ID	IPS特征的编号

字段	描述
Direction	IPS特征的方向属性，包括如下取值： • any：表示一个会话的两个方向 • To-server：一个会话的客户端到服务器方向 • To-client：一个会话的服务器到客户端方向
Severity	IPS特征的攻击严重程度属性，严重程度从低到高分为四个级别：Low、Medium、High、Critical
Fidelity	IPS特征的可信度属性，可信度从低到高分为三个级别：Low、Medium、High
Category	IPS特征的攻击类别名称
Protocol	IPS特征的协议属性

1.1.5 display ips signature user-defined parse-failed

display ips signature user-defined parse-failed 命令用来显示 IPS 自定义特征解析失败的信息。

【命令】

display ips signature user-defined parse-failed

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

此命令用于查看 IPS 自定义特征解析失败的原因以及修改建议。

【举例】

显示 IPS 自定义特征解析失败的信息。

```
<Sysname> display ips signature user-defined parse-failed
LineNo  SID         Information
1       None        Error: Invalid actions.
                    Tip: Only actions {alert|drop|pass|reject|sdrop|log} are supported
2       1010082     Error: Invalid signature ID.
                    Tip: The signature ID must be in the range of 1 to 536870912
3       1010083     Error: Invalid protocol.
                    Tip: Only protocols {tcp|udp|icmp|ip} are supported
4       1010084     Error: Invalid direction.
                    Tip: Only directions {'<>'|'->'} are supported
```

表1-3 display ips signature user-defined parse-failed 命令显示信息描述表

字段	描述
LineNo	Snort规则文件中的行号
SID	自定义特征的编号
Information	自定义特征解析失败的信息，包括如下取值： • Error：表示自定义特征解析失败的原因 • Tip：表示 Snort 规则文件内容的修改建议

【相关命令】

- **ips signature import snort**

1.1.6 display ips signature { pre-defined | user-defined }

display ips signature { **pre-defined** | **user-defined** }命令用来显示 IPS 特征的详细信息。

【命令】

display ips signature { **pre-defined** | **user-defined** } *signature-id*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

pre-defined：显示预定义 IPS 特征的详细信息。

user-defined：显示自定义 IPS 特征的详细信息。

signature-id：指定 IPS 特征的编号，其中，预定义 IPS 特征的取值范围为 1～536870911；自定义 IPS 特征的取值范围为 536870913～1073741823。

【举例】

显示编号为 1 的预定义 IPS 特征的详细信息。

```
<Sysname> display ips signature pre-defined 1
 Type         : Pre-defined
 Signature ID: 1
 Status       : Enabled
 Action       : Reset & Logging
 Name         : GNU_Bash_CVE-2014-6271_Remote_Code_Execution_Vulnerability
 Protocol     : TCP
 Severity     : High
 Fidelity     : Medium
```

```
 Direction   : To-server
 Category    : Vulnerability
 Reference   : CVE-2014-6271;
 Description : GNU Bash through 4.3 processes trailing strings after function definitions
in the values of environment variables, which allows remote attackers to execute arbitrary
code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature
in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed
by unspecified DHCP clients, and other situations in which setting the environment occurs
across a privilege boundary from Bash execution, aka \"ShellShock.\" NOTE: the original fix
for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that
is still present after the incorrect fix.
```

表1-4 display ips signature { pre-defined | user-defined }命令显示信息描述表

字段	描述
Type	IPS特征的类型，包括如下取值： • Pre：表示预定义特征 • User：表示自定义特征
Signature ID	IPS特征的编号
Status	IPS特征的状态，包括如下取值： • Enabled：表示此特征已生效 • Disabled：表示此特未生效
Action	对报文的处理动作，包括如下取值： • Block-source：表示阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单 • Drop：表示丢弃符合特征的报文 • Permit：表示允许符合特征的报文通过 • Reset：表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 • Capture：表示捕获符合特征的报文 • Logging：表示对符合特征的报文生成日志
Name	IPS特征的名称
Protocol	IPS特征的协议属性
Severity	IPS特征的攻击严重程度属性，严重程度从低到高分为四个级别：Low、Medium、High、Critical
Fidelity	IPS特征的可信度属性，可信度从低到高分为三个级别：Low、Medium、High
Direction	IPS特征的方向属性，包括如下取值： • any：表示一个会话的两个方向 • To-server：一个会话的客户端到服务器方向 • To-client：一个会话的服务器到客户端方向
Category	IPS特征的攻击类别名称
Reference	IPS特征的参考信息
Description	IPS特征的描述信息

1.1.7 display ips signature information

display ips signature information 命令用来显示 IPS 特征库信息。

【命令】

display ips signature information

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 IPS 特征库信息。

```
<Sysname> display ips signature information
IPS signature library information:
Type     SigVersion         ReleaseTime               Size
Current  1.02               Fri Sep 13 09:05:35 2014  71594
Last     -                  -                         -
Factory  1.00               Fri Sep 11 09:05:35 2014  71394
```

表1-5 display ips signature information 命令显示信息描述表

字段	描述
Type	IPS特征库版本，包括如下取值： • Current：表示当前版本 • Last：表示上一版本 • Factory：表示出厂版本
SigVersion	IPS特征库版本号
ReleaseTime	IPS特征库发布时间
Size	IPS特征库文件大小，单位是Bytes

1.1.8 ips apply policy

ips apply policy 命令用来在 DPI 应用 profile 中引用 IPS 策略。

undo ips apply policy 命令用来删除引用的 IPS 策略。

【命令】

ips apply policy *policy-name* **mode** { **alert** | **protect** }

undo ips apply policy

【缺省情况】

DPI 应用 profile 中没有引用 IPS 策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示 IPS 策略名称，为 1～63 个字符的字符串，不区分大小写。

mode：表示 IPS 策略的模式。

alert：告警模式，表示报文匹配上该 IPS 策略中的特征后，仅可以生成日志或捕获报文，但其他动作均不能生效。

protect：保护模式，表示报文匹配上该 IPS 策略中的特征后，设备按照特征的动作对该报文进行处理。

【使用指导】

一个 DPI 应用 profile 视图下只能引用一个 IPS 策略。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 sec 的 DPI 应用 profile 下引用 IPS 策略 ips1，且配置 IPS 模式为保护模式。

```
<Sysname> system-view
[Sysname] app-profile sec
[Sysname-app-profile-sec] ips apply policy ips1 mode protect
```

【相关命令】

- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **ips policy**

1.1.9 ips parameter-profile

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** 命令用来配置 IPS 引用应用层检查引擎动作参数 profile。

undo ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** 命令用来取消 IPS 引用的应用层检查引擎动作参数 profile。

【命令】

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** *parameter-name*

undo ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile**

【缺省情况】

IPS 未引用应用层检查引擎动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source：表示设置 IPS 源阻断动作的参数。

capture：表示设置 IPS 捕获动作的参数。

email：表示设置 IPS 邮件动作的参数。

logging：表示设置 IPS 日志动作的参数。

redirect：表示设置 IPS 重定向动作的参数。

parameter-profile *parameter-name*：指定 IPS 动作引用的应用层检测引擎动作参数 profile。*parameter-name* 表示动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

每类 IPS 动作的具体执行参数由应用层检测引擎动作参数 profile 来定义，该 profile 的具体配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

如果 IPS 引用的应用层检测引擎动作参数 profile 不存在或没有引用，则使用系统各类动作参数的缺省值。

【举例】

创建名称为 ips1 的应用层检测引擎源阻断动作参数 profile，配置其阻断源 IP 地址的时长为 1111 秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile ips1
[Sysname-inspect-block-source-ips1] block-period 1111
[Sysname-inspect-block-source-ips1] quit
```

配置 IPS 引用名称为 ips1 的应用层检查引擎源阻断动作参数 profile。

```
[Sysname] ips block-source parameter-profile ips1
```

【相关命令】

- **inspect block-source parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect capture parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect logging parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect email parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect redirect parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）

1.1.10 ips policy

ips policy 命令用来创建 IPS 策略，并进入 IPS 策略视图。如果指定的 IPS 策略已经存在，则直接进入 IPS 策略视图。

undo ips policy 命令用来删除指定的 IPS 策略。

【命令】

ips policy *policy-name*

undo ips policy *policy-name*

【缺省情况】

存在一个缺省 IPS 策略，名称为 default。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示 IPS 策略名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

设备上存在一个名称为 default 的缺省 IPS 策略，缺省 IPS 策略和自定义 IPS 策略都使用当前系统中的所有 IPS 特征，新增 IPS 特征会自动添加到所有策略下。但是缺省 IPS 策略中的 IPS 特征的动作属性和生效状态属性不能被修改。

【举例】

创建一个名称为 ips1 的 IPS 策略，并进入 IPS 策略视图。

```
<Sysname> system-view
[Sysname] ips policy ips1
[Sysname-ips-policy-ips1]
```

1.1.11 ips signature auto-update

ips signature auto-update 命令用来开启定期自动在线升级 IPS 特征库功能，并进入自动升级配置视图。

undo ips signature auto-update 命令用来关闭定期自动在线升级 IPS 特征库功能。

【命令】

ips signature auto-update

undo ips signature auto-update

【缺省情况】

定期自动在线升级 IPS 特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问 H3C 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 IPS 特征库进行升级。

【举例】

开启定期自动在线升级 IPS 特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate]
```

【相关命令】

- **update schedule**

1.1.12 ips signature auto-update-now

ips signature auto-update-now 命令用来立即自动在线升级 IPS 特征库。

【命令】

ips signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行此命令后，将立即自动升级设备上的 IPS 特征库，且会备份当前的 IPS 特征库文件。此命令的生效与否，与是否开启了定期自动升级 IPS 特征库功能无关。

当管理员发现 H3C 官方网站上的特征库服务专区中的 IPS 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 IPS 特征库版本。

【举例】

立即自动在线升级 IPS 特征库版本。

```
<Sysname> system-view
[Sysname] ips signature auto-update-now
```

1.1.13 ips signature import snort

ips signature import snort 命令用来导入自定义 IPS 特征。

【命令】

ips signature import snort *file-path*

【缺省情况】

不存在自定义 IPS 特征。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

file-path：自定义 IPS 特征库文件的 URL，为 1～255 个字符的字符串。

【使用指导】

当需要的 IPS 特征在设备当前 IPS 特征库中不存在时，可通过编辑 Snort 格式的 IPS 特征文件，并将其导入设备中来生成所需的 IPS 特征。导入的 IPS 特征文件内容会自动覆盖系统中所有的自定义 IPS 特征。可通过 **display ips signature user-defined** 命令查看导入的 IPS 特征信息。

管理员可以采用如下几种方式导入自定义 IPS 特征库文件。

- 本地方式：使用本地保存的自定义 IPS 特征库文件导入。
- FTP/TFTP 方式：通过 FTP 或 TFTP 方式下载远程服务器上保存的自定义 IPS 特征库文件，并导入到系统中。

参数 *file-path* 的取值与自定义 IPS 特征库文件导入的操作方式有关。采用本地方式时参数 *file-path* 取值请参见表 1-6；采用 FTP/TFTP 方式时参数 *file-path* 取值请参见表 1-7。

表1-6 采用本地方式时参数 *file-path* 取值说明表

导入方式	参数 *file-path* 取值	说明
自定义IPS特征库文件的存储位置与当前工作路径一致	*filename*	可以执行**pwd**命令查看当前工作路径 有关**pwd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
自定义IPS特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	*path/ filename*	-
自定义IPS特征库文件的存储位置与当前工作路径不在相同存储介质上	*path/ filename*	需要先执行**cd**命令将工作路径切换至自定义IPS特征库文件所在存储介质的根目录下，再指定自定义IPS特征库文件的相对路径 有关**cd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-7 采用 FTP/TFTP 方式时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
自定义IPS特征库文件存储在开启FTP服务的远程服务器上	*ftp://username:password@server/filename*	*username*为登录FTP服务器的用户名，*password*为登录FTP服务器的密码，*server*为FTP服务器的IP地址或主机名 当FTP用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”

升级场景	参数 *file-path* 取值	说明
自定义IPS特征库文件存储在开启TFTP服务的远程服务器上	*tftp://server/filename*	*server*为TFTP服务器的IP地址或主机名

编辑 Snort 格式的 IPS 特征文件需要注意的是：

Snort 文件需要遵循 Snort 公司的语法。

Snort 规则的 SID 取值范围为 1～536870911，若超出此范围，则规则无效。

编辑 Snort 规则时，必须配置 msg 字段，否则 IPS 系统日志中威胁名称字段是空的。

当用户自定义 Snort 规则中的应用无法被识别时，报文无法成功匹配该规则。

【相关命令】

- **display ips signature user-defined**
- **ips signature remove snort**

【举例】

采用 TFTP 方式，将自定义 Snort 格式的 IPS 特征库文件导入设备生成自定义 IPS 特征，自定义 Snort 格式的 IPS 特征库文件的远程路径为 tftp://192.168.0.1/snort.rules。

```
<Sysname> system-view
[Sysname] ips signature import snort tftp://192.168.0.1/snort.rules
```

1.1.14 ips signature remove snort

ips signature remove snort 命令用来删除导入的所有自定义 IPS 特征。

【命令】

ips signature remove snort

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

删除导入的所有自定义 IPS 特征。

```
<Sysname> system-view
[Sysname] ips signature remove snort
```

【相关命令】

- **ips signature import snort**

1.1.15 ips signature rollback

ips signature rollback 命令用来回滚 IPS 特征库。

【命令】

ips signature rollback { **factory** | **last** }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory：表示 IPS 特征库的出厂版本。

last：表示 IPS 特征库的上一版本。

【使用指导】

IPS 特征库回滚是指将当前的 IPS 特征库版本回滚到指定的版本。如果管理员发现设备当前 IPS 特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前 IPS 特征库版本进行回滚。目前支持将设备中的 IPS 过滤特征库版本回滚到出厂版本和上一版本。

IPS 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 IPS 特征库是 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。

【举例】

配置 IPS 特征库回滚到上一版本。

```
<Sysname> system-view
[Sysname] ips signature rollback last
```

1.1.16 ips signature update

ips signature update 命令用来手动离线升级 IPS 特征库。

【命令】

ips signature update [**override-current**] *file-path*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

override-current：表示覆盖当前版本的特征库文件。如果不指定本参数，则表示当前特征库在升级之后作为备份特征库保存在设备上。

file-path：指定特征库文件的路径，为 1～255 个字符的字符串。

【使用指导】

如果设备不能访问 H3C 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 IPS 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 IPS 特征库版本。特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。
- 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 IPS 特征库版本。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见表 1-8；FTP/TFTP 升级时参数 *file-path* 取值请参见表 1-9。

表1-8 本地升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件的存储位置与当前工作路径一致	*filename*	可以执行**pwd**命令查看当前工作路径 有关**pwd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	*path/ filename*	-
特征库文件的存储位置与当前工作路径不在相同存储介质上	*path/ filename*	需要先执行**cd**命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关**cd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-9 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件存储在开启FTP服务的远程服务器上	*ftp://username:password@server/filename*	*username*为登录FTP服务器的用户名，*password*为登录FTP服务器的密码，*server*为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启TFTP服务的远程服务器上	*tftp://server/filename*	*server*为TFTP服务器的IP地址或主机名

说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级 IPS 特征库，且采用 TFTP 方式，IPS 特征库文件的远程路径为 tftp://192.168.0.10/ips-1.0.2-en.dat。

```
<Sysname> system-view
[Sysname] ips signature update tftp://192.168.0.10/ips-1.0.2-en.dat
```

配置手动离线升级 IPS 特征库，且采用 FTP 方式，IPS 特征库文件的远程路径为 ftp://192.168.0.10/ips-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
[Sysname] ips signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/ips-1.0.2-en.dat
```

配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为 cfa0:/ips-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
[Sysname] ips signature update ips-1.0.23-en.dat
```

配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为 cfa0:/dpi/ips-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
[Sysname] ips signature update dpi/ips-1.0.23-en.dat
```

配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为 cfb0:/dpi/ips-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
<Sysname> system
[Sysname] ips signature update dpi/ips-1.0.23-en.dat
```

1.1.17 object-dir

object-dir 命令用来配置筛选 IPS 特征的方向属性。

undo object-dir 命令用来恢复缺省情况。

【命令】

object-dir { **client** | **server** } *

undo object-dir

【缺省情况】

IPS 策略匹配所有方向上的对象。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

client：表示从服务器到客户端方向上的对象。

server：表示从客户端到服务器方向上的对象。

【使用指导】

可通过配置方向属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个方向，只要符合其中一个，具有该方向属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中仅保护从服务器到客户端方向上的对象。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] object-dir client
```

1.1.18 override-current

override-current 命令用来配置定期自动在线升级 IPS 特征库时覆盖当前的特征文件。

undo override-current 命令用来恢复缺省情况。

【命令】

override-current

undo override-current

【缺省情况】

定期自动在线升级 IPS 特征库时不会覆盖当前的特征库文件，而是同时将当前的特征库文件备份为上一版本。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

可以通过开启此功能解决升级 IPS 特征库时设备内存不足的问题。在设备剩余内存充裕的情况下，不建议配置该功能，因为 IPS 特征库升级时，如果没有备份当前特征库文件，则不能回滚到上一版本。

配置此功能后定期自动在线升级 IPS 特征库时不会将当前的特征库文件备份为上一版本。

【举例】

配置定期自动在线升级 IPS 特征库时覆盖当前的特征文件。

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate] override-current
```

【相关命令】

- **ips signature auto-update**

1.1.19 protect-target

protect-target 命令用来配置筛选 IPS 特征的保护对象属性。

undo protect-target 命令用来删除筛选 IPS 特征的保护对象属性。

【命令】

protect-target { *target* [*subtarget*] | **all** }

undo protect-target { *target* [*subtarget*] | **all** }

【缺省情况】

IPS 策略匹配所有保护对象的特征。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

target：表示保护对象分类名称。

subtarget：表示保护对象分类中的子对象名称。若不指定本参数，则表示保护某对象分类中的所有子对象。

all：表示所有保护对象。

【使用指导】

可通过配置保护对象属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个保护对象。只要符合其中一个，具有该保护对象属性的特征将会被筛选出来。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的保护对象为 WebServer 中 WebLogic 子对象。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] protected-target WebServer WebLogic
```

1.1.20 severity-level

severity-level 命令用来配置筛选 IPS 特征的严重级别属性。

undo severity-level 命令用来恢复缺省情况。

【命令】

severity-level { **critical** | **high** | **low** | **medium** } *

undo severity-level

【缺省情况】

IPS 策略匹配所有严重级别的特征。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

critical：表示严重级别最高。

high：表示严重级别高。

low：表示严重级别低。

medium：表示严重级别一般。

【使用指导】

可通过配置严重级别属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个严重级别，只要符合其中一个，具有该严重级别属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的严重级别为 critical 和 medium。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] severity-level critical medium
```

1.1.21 signature override

signature override 命令用来修改 IPS 策略中指定特征的动作和状态。

undo signature override 命令用来恢复 IPS 策略中指定特征属性中的动作和状态。

【命令】

signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }

undo signature override { **pre-defined** | **user-defined** } *signature-id*

【缺省情况】

预定义 IPS 特征使用系统预定义的状态和动作，自定义 IPS 特征的动作和状态在管理员导入的特征库文件中定义。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

pre-defined：表示预定义的 IPS 特征。

user-defined：表示自定义的 IPS 特征。

signature-id：IPS 特征的编号，取值范围为 1～4294967295。

disable：表示禁用此 IPS 特征。在某些网络环境中，如果一些 IPS 特征暂时不会被用到，而且又不想将其从 IPS 策略中删除时，可以使用 **disable** 参数来禁用这些规则。

enable：表示启用此 IPS 特征。

block-source：表示源阻断，该动作阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop：表示丢弃报文。

permit：表示允许报文通过。

redirect：表示把符合特征的报文重定向到指定的 Web 页面上。

reset：表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture：表示捕获报文。

logging：表示生成报文日志。

【使用指导】

缺省情况下，IPS 策略将使用当前设备上所有处于生效状态的 IPS 特征与报文进行匹配，并对匹配成功的报文执行 IPS 特征属性中的动作。管理员可以根据实际网络需求，修改 IPS 策略中指定特征的动作和状态。如果报文与该 IPS 特征匹配成功，则对报文执行该特征的动作。

缺省 IPS 策略中的 IPS 特征的动作和生效状态不能被修改。当 IPS 策略中的 IPS 特征被禁用后，此 IPS 特征对用户报文不生效。

在同一个 IPS 策略视图中对同一 IPS 特征多次执行此命令，最后一次执行的命令生效。

【举例】

在名称为 ips1 的 IPS 策略中，配置编号为 2 的预定义 IPS 特征的状态为开启，动作为丢弃和捕获报文，并生成日志信息。

```
<Sysname> system-view
[Sysname] ips policy ips1
[Sysname-ips-policy-ips1] signature override pre-defined 2 enable drop capture logging
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **ips parameter-profile**
- **ips policy**
- **signature override all**

1.1.22 signature override all

signature override all 命令用来配置 IPS 策略中所有特征的统一动作。

undo signature override all 命令用来恢复缺省情况。

【命令】

signature override all { { **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging** } *

undo signature override all

【缺省情况】

IPS 策略执行特征属性中的动作。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source：表示源阻断，该动作阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop：表示丢弃报文。

permit：表示允许报文通过。

redirect：表示把符合特征的报文重定向到指定的 Web 页面上。

reset：表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture：表示捕获报文。

logging：表示生成报文日志。

【使用指导】

如果在 IPS 策略中为所有特征配置了统一动作，则设备将根据该动作对与此策略中特征匹配成功的报文进行处理。否则，设备将根据特征属性中的动作对报文进行处理。

如果在 IPS 策略中修改了指定特征的动作，则无论 IPS 策略是否为所有特征配置了动作，设备都将根据修改后的特征的动作对与报文进行处理。

【举例】

配置名称为 text 的 IPS 策略中所有特征的统一动作为丢弃，并生成日志信息和捕获报文。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] signature override all drop logging capture
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **ips parameter-profile**
- **signature override**

1.1.23 update schedule

update schedule 命令用来配置定期自动在线升级 IPS 特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

【缺省情况】

设备在每天 01:00:00 至 03:00:00 之间自动在线升级 IPS 特征库。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【参数】

daily：表示自动升级周期为每天。

weekly：表示以一周为周期，在指定的一天进行自动升级。

fri：表示星期五。

mon：表示星期一。

sat：表示星期六。

sun：表示星期日。

thu：表示星期四。

tue：表示星期二。

wed：表示星期三。

start-time *time*：指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

tingle *minutes*：指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置 IPS 特征库的定期自动在线升级时间为每周一 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

【相关命令】

- **ips signature auto-update**

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：

型号	特性	描述
F1000-E-G2/F1000-A-G2/F1000-S-G2/F1000-C-G2	URL过滤	支持
F100-E-G2/F100-A-G2/F100-M-G2/F100-S-G2/F100-C-G2		• F100-M-G2/F100-S-G2/F100-C-G2：不支持 • F100-E-G2/F100-A-G2：支持
F1000-C-EI/F100-E-EI/F100-A-EI/F100-C-EI/F100-A-SI		• F100-C-EI：不支持 • F1000-C-EI/F100-E-EI/F100-A-EI/F100-A-SI：支持
F100-C-HI/F100-S-HI/F100-A-HI/F1000-C-HI		• F100-A-HI/F1000-C-HI：支持 • F100-C-HI/F100-S-HI：不支持
F1000-C8180/F1000-C8170/F1000-C8160/F1000-C8150/F1000-C8130/F1000-C8120		• F1000-C8180/F1000-C8170/F1000-C8160：支持 • F1000-C8150/F1000-C8130/F1000-C8120：不支持
F100-C80-WiNet/F100-C60-WiNet		不支持

1.1 URL过滤配置命令

1.1.1 add

add 命令用来向 URL 过滤策略中添加黑/白名单规则。

undo add 命令用来删除 URL 过滤策略中指定的或所有黑/白名单规则。

【命令】

add { **blacklist** | **whitelist** } [*id*] **host** { **regex** *host-regex* | **text** *host-name* } [**uri** { **regex** *uri-regex* | **text** *uri-name* }]

undo add { **blacklist** | **whitelist** } { *id* | **all** }

【缺省情况】

URL 过滤策略中不存在黑/白名单规则。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

blacklist：表示 URL 过滤策略的黑名单规则。

whitelist：表示 URL 过滤策略的白名单规则。

id：表示黑/白名单规则的编号，取值范围为 1～65535。若未指定本参数，系统将从 1 开始，自动分配一个大于现有最大编号的最小编号，步长为 1。若新编号超出了编号上限 65535，则选择当前未使用的最小编号作为新的编号。

host：表示匹配 URL 中的主机名字段。

uri：表示匹配 URL 中的 URI 字段。

regex *regex*：表示使用正则表达式对主机名和 URI 字段进行模糊匹配。*regex* 是正则表达式，主机名规则的取值范围为 4～224 个字符的字符串，不区分大小写，只能以字母、数字和下划线开头；URI 规则的取值范围为 4～253 个字符的字符串，区分大小写，只能以字母、数字和下划线开头。

text *string*：表示使用文本对主机名和 URI 字段进行精确匹配。*string* 是指定的主机名或 URI 规则字符串，主机名规则的取值范围为 3～224 个字符的字符串，不区分大小写主机名只能是字母、数字、下划线“_”、连接符“-”、冒号“：”、左方括号“[”、右方括号“]”和点号“.”，但 URI 无此限制；URI 规则的取值范围为 3～255 个字符的字符串，区分大小写。

all：表示所有的黑/白名单规则。

【使用指导】

URL 过滤黑/白名单规则功能根据应层的信息进行 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。

【举例】

在 URL 过滤策略 news 中，添加一条黑名单规则，使用字符串 games.com 对主机名字段进行精确匹配。

```
<Sysname> system-view
[Sysname] url-filter policy news
[System-url-filter-policy-news] add blacklist 1 host text games.com
```

添加一条白名单规则，并使用字符串 sina.com 对主机名字段进行精确匹配。

```
[System-url-filter-policy-news] add whitelist 1 host text sina.com
```

1.1.2 category action

category action 命令用来配置 URL 过滤分类动作。

undo category action 命令用来删除指定的 URL 过滤分类动作。

【命令】

category *category-name* **action** { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

undo category *category-name*

【缺省情况】

不存在 URL 过滤分类动作。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

category-name：指定 URL 过滤分类名称，包括预定义和自定义的 URL 过滤分类名称，为 1～63 个字符的字符串，不区分大小写。

action：表示对匹配上此 URL 过滤分类中的任何一条规则的报文所采取的动作。

block-source：表示阻断报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名过滤单功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop：表示丢弃报文。

permit：表示允许报文通过。

redirect：表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。

reset：表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。

logging：表示生成报文日志。

parameter-profile *parameter-name*：指定引用的动作参数。*parameter-name* 是动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。如果不指定该参数或指定的参数不存在，则使用动作的缺省参数。这里引用的动作参数是应用层检测引擎中配置的动作参数，有关应用层检测引擎中动作参数的详细配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【使用指导】

URL 过滤功能对报文的处理过程如下：

- 如果报文匹配上该 URL 过滤分类中的任何一条规则，则设备将会根据该 URL 过滤分类绑定的动作对此报文进行处理。
- 如果报文没有匹配上该 URL 过滤分类中的任何规则，但是配置了 **default-action** 命令，则设备将根据 URL 过滤策略中配置的缺省动作来对此报文进行处理。
- 如果报文没有匹配上该 URL 过滤分类中的任何规则，且也没有配置 **default-action** 命令，则设备直接允许此报文通过。

【举例】

在 URL 过滤策略 news 中，配置 URL 过滤分类 sina 的动作为丢弃。

```
<Sysname> system-view
[Sysname] url-filter policy news
[System-url-filter-policy-news] category sina action drop
```

【相关命令】

- **inspect block-source parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect redirect parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **url-filter category**
- **url-filter policy**

1.1.3 cloud-query enable

cloud-query enable 命令用来开启 URL 过滤分类云端查询功能。

undo cloud-query enable 命令用来关闭 URL 过滤分类云端查询功能。

【命令】

cloud-query enable

undo cloud-query enable

【缺省情况】

URL 过滤分类云端查询功能处于关闭状态。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在 URL 过滤策略中开启 URL 过滤分类云端查询功能后，如果流经设备 HTTP 报文中的 URL 与该 URL 过滤策略中的过滤规则匹配失败，则此 URL 将会被发向云端 URL 过滤分类服务器进行查询。云端 URL 过滤分类服务器响应该请求，并向设备发送查询结果，该结果中包含了 URL 过滤规则及其所属的分类名称，设备根据该结果执行相应的分类处理动作。如果云端返回的分类在设备上没有与其对应的分类动作或者云端 URL 查询失败，则设备将对此报文执行 URL 过滤策略中的缺省动作。

【举例】

在 URL 过滤策略中开启 URL 过滤分类云端查询功能。

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] cloud-query enable
```

【相关命令】

- **url-filter policy**

1.1.4 default-action

default-action 命令用来配置 URL 过滤策略的缺省动作。

undo default-action 命令用来恢复缺省情况。

【命令】

default-action { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect** **parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

undo default-action

【缺省情况】

URL 过滤策略中不存在缺省动作。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source：表示阻断报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名过滤单功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop：表示丢弃报文。

permit：表示允许报文通过。

redirect：表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。

reset：表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。

logging：表示生成报文日志动作。

parameter-profile *parameter-name*：指定引用的动作参数。*parameter-name* 是动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。如果不指定该参数或指定的参数不存在，则使用动作的缺省参数。这里引用的动作参数是应用层检测引擎中配置的动作参数，有关应用层检测引擎中动作参数的详细配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【使用指导】

配置此命令后，当报文没有匹配上 URL 过滤策略中的规则时，设备将根据 URL 过滤策略的缺省动作对此报文进行处理。

【举例】

在 URL 过滤策略 news 中，配置缺省动作为丢弃。

```
<Sysname> system-view
[Sysname] url-filter policy cmcc
[Sysname-url-filter-policy-cmcc] default-action drop
```

【相关命令】

- **inspect block-source parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect redirect parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **url-filter policy**

1.1.5 description

description 命令用来配置 URL 过滤分类的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

自定义的 URL 过滤分类中不存在描述信息。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：URL 过滤分类的描述信息，为 1～255 个字符的字符串，可以包含空格，不区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别 URL 过滤分类的作用，有利于后期维护。

【举例】

配置 URL 过滤分类 news 的描述信息为 News information。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] description News information
```

1.1.6 display url-filter cache

display url-filter cache 命令行用来查看 URL 过滤缓存中的信息。

【命令】

display url-filter cache [**existence** { **eq** | **lt** | **gt** } *existence-time* | **category** *category-name* | **hitcount** { **eq** | **lt** | **gt** } *hit-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

existence *existence-time*：指定缓存 URL 过滤规则的保存时间，取值范围为 0～4294967295，单位为秒。

eq：表示等于指定的保存时间。

lt：表示小于指定的保存时间。

gt：表示大于指定的保存时间。

category *category-name*：指定 URL 过滤分类，*category-name* 为 URL 过滤分类名称。

hitcount *hitnumber*：指定 URL 过滤规则命中次数，取值范围为 0～4294967295，单位为次。

eq：表示等于指定的命中次数。

lt：表示小于指定的命中次数。

gt：表示大于指定的命中次数。

【举例】

查看 URL 过滤缓存中的信息。

```
<Sysname> display url-filter cache
          URL: sina.com
     Category: Unknown
     Hitcount: 20
    Existence: 7200 seconds (cached on 2014/11/12 at 15:00:00)

          URL: baidu.com
     Category: Search
     Hitcount: 20
    Existence: 3600 seconds (cached on 2014/11/12 at 16:00:00)
```

表1-1 display url-filter cache 命令显示信息描述表

字段	描述
URL	缓存中URL过滤规则的内容
Category	URL过滤分类名称，这里是从服务器学习到名称，若还没有查询到，则显示为Unknown
Hitcount	该URL过滤规则被命中的次数
Existence	该URL过滤规则在缓存中的时间，同时显示首次进入缓存的UTC时间

【相关命令】

- **url-filter category**

1.1.7 display url-filter category

display url-filter category 命令用来查看 URL 过滤分类信息。

【命令】

display url-filter category [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

verbose：显示 URL 过滤分类的详细信息。如果不指定该参数，则显示 URL 过滤分类的摘要信息。

【举例】

查看 URL 过滤分类信息。

```
<Sysname> display url-filter category
Url-filter categories total
      Predefine category count : 53
          Predefine rule count : 2000
    User define category count : 5
        User define rule count : 4
Url-filter categories
           Name : 23
           Name : 24
           Name : 33
           Name : Pre-AdvertisementsAndPop-Ups
           Name : Pre-AlcoholAndTobacco
           Name : Pre-Anonymizers
           Name : Pre-Arts
           Name : Pre-Business
           Name : Pre-Chat
           Name : Pre-ComputersAndTechnology
           Name : Pre-CriminalActivity
           Name : Pre-Cults
           Name : Pre-DatingAndPersonals
           Name : Pre-DownloadSites
           Name : Pre-Education
           Name : Pre-Entertainment
           Name : Pre-FashionAndBeauty
---- More ----
```

查看 URL 过滤分类的详细信息。

```
<Sysname> display url-filter category verbose
Url-filter categories total
      Predefine category count : 53
          Predefine rule count : 2000
    User define category count : 5
        User define rule count : 4
Url-filter categories
```

```
          Name : 23
          Type : User defined
      Critical : 1001
     Rule count : 1
    Description :
          Name : 24
          Type : User defined
      Critical : 1002
     Rule count : 1
    Description :
          Name : Pre-AdvertisementsAndPop-Ups
          Type : Predefined
      Critical : 300
     Rule count : 32
    Description : Sites that provide advertising graphics or other ad content fi
                  les such as banners and pop-ups.
          Name : Pre-AlcoholAndTobacco
          Type : Predefined
      Critical : 960
     Rule count : 7
    Description : Sites that promote or sell alcohol- or tobacco-related product
                  s or services.
---- More ----
```

表1-2 display url-filter category 命令显示信息描述表

字段	描述
URL-filter categories total	设备中URL过滤分类总数，包括预定义的分类和自定义的分类
Predefine category count	预定义URL过滤分类数目
Predefine rule count	预定义URL过滤规则数目
User define category count	自定义URL过滤分类数目
User define rule count	自定义URL过滤规则数目
URL-filter categories	URL过滤分类表项
Name	URL过滤分类名称
Type	URL过滤分类类型，包括如下取值： • Predefined：预定义分类 • User defined：自定义分类
Critical	URL过滤严重级别
Description	URL过滤分类描述信息

1.1.8 display url-filter signature information

display url-filter signature information 查看 URL 过滤特征库信息。

【命令】

display url-filter signature information

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

查看 URL 过滤特征库信息。

```
<Sysname> display url-filter signature information
URL filter signature library information:
Type      SigVersion         ReleaseTime               Size
Current   1.0.0              Wed Jan 21 06:43:53 2015  36096
(null)    -                  -                         -
Factory   1.0.0              Wed Jan 21 06:43:53 2015  36096
```

表1-3 display url-filter signature information 命令显示信息描述表

字段	描述
Type	URL过滤特征库版本，包括如下取值： • Current：当前版本 • Last：上一版本 • Factory：出厂版本
SigVersion	URL过滤特征库版本号
ReleaseTime	URL过滤特征库发布时间
Size	URL过滤特征库文件大小，单位是Bytes

1.1.9 display url-filter statistics

display url-filter statistics 命令用来查看 URL 过滤的统计信息。

【命令】

display url-filter statistics

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 URL 规则命中统计信息。

```
<Sysname> display url-filter statistics
Total HTTP requests                          : 0
Total permitted HTTP requests                : 0
Total denied HTTP requests                   : 0
Requests that matched the blacklist          : 0
Requests that matched the whitelist          : 0
Requests that matched a user-defined rule    : 0
Requests that matched a predefined rule      : 0
Requests that matched a cached rule          : 0
Requests that matched the default action     : 0
Predefined URL filtering rules               : 2000
--------------------------------------------------------------
```

表1-4 display url-filter statistics 命令显示信息描述表

字段	描述
Total HTTP requests	HTTP报文总数
Total permitted HTTP requests	HTTP报文放行个数
Total denied HTTP requests	HTTP报文拒绝个数
Requests that matched the blacklist	黑名单规则命中数
Requests that matched the whitelist	白名单规则命中数
Requests that matched a user-defined rule	自定义规则命中数
Requests that matched a predefined rule	预定义规则命中数
Requests that matched a cached rule	缓存规则命中数
Requests that matched the default action	默认动作命中数
Predefined URL filtering rules	预定义规则数量

1.1.10 include pre-defined

include pre-defined 命令用来添加预定义 URL 过滤分类中的规则。

undo include pre-defined 命令用来恢复缺省情况。

【命令】

include pre-defined *category-name*

undo include pre-defined

【缺省情况】

URL 过滤分类中未添加预定义 URL 过滤分类中的规则。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

category-name：表示预定义 URL 过滤分类的名称，为 1～63 个字符的字符串，区分大小写。指定的预定义 URL 过滤分类必须已存在。

【使用指导】

当新建的 URL 过滤分类中所需的规则与已存在的预定义 URL 过滤分类中的规则比较相似时，可通过此命令灵活、快速的创建 URL 过滤分类。

一个 URL 过滤分类下只能添加一个预定义 URL 过滤分类。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 news 的 URL 过滤分类中加预定义 URL 过滤分类 pre-Arts 中的规则。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] include pre-defined pre-Arts
```

1.1.11 rename (URL filtering category view)

rename 命令用来重命名 URL 过滤分类，并进入新的 URL 过滤分类视图。

【命令】

rename *new-name*

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

new-name：表示新的 URL 过滤分类的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

原有 URL 过滤分类的名称被修改后，URL 过滤策略中引用的同名 URL 过滤分类的名称也会被同步修改。

【举例】

把名称为 news 的 URL 过滤分类重命名为 hello，并进入新的 URL 过滤分类视图。

```
<Sysname> system-view
[Sysname] url-filter category news
```

```
[Sysname-url-filter-category-news] rename hello
[Sysname-url-filter-category-hello]
```

1.1.12 rename (URL filtering policy view)

rename 命令用来重命名 URL 过滤策略，并进入新的 URL 过滤策略视图。

【命令】

rename *new-name*

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

new-name：表示新的 URL 过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

原有 URL 过滤策略的名称被修改后，DPI 应用 profile 中引用的同名 URL 过滤策略的名称也会被同步修改。

【举例】

把名称为 news 的 URL 过滤策略重命名为 hello，并进入新的 URL 过滤策略视图。

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] rename hello
[Sysname-url-filter-policy-hello]
```

1.1.13 reset url-filter statistics

reset url-filter statistics 命令用来清除 URL 过滤的统计信息。

【命令】

reset url-filter statistics

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【举例】

清除 URL 过滤的统计信息。

```
<Sysname> reset url-filter statistics
```

【相关命令】

- **display url-filter statistics**

1.1.14 rule

rule 命令用来在自定义 URL 过滤分类中创建 URL 过滤规则。

undo rule 命令用来在自定义 URL 过滤分类中删除指定的 URL 过滤规则。

【命令】

rule *rule-id* **host** { **regex** *regex* | **text** *string* } [**uri** { **regex** *regex* | **text** *string* }]

undo rule *rule-id*

【缺省情况】

自定义 URL 过滤分类中不存在 URL 过滤规则。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id：指定 URL 过滤规则编号，取值范围为 1～65535。

host：表示 URL 过滤规则匹配 URL 中的主机名字段。

uri：表示 URL 过滤规则匹配 URL 中的 URI 字段。

regex *regex*：表示 URL 过滤规则使用正则表达式对主机名和 URI 字段进行模糊匹配。*regex* 表示正则表达式，主机名正则表达式的取值范围为 4～224 个字符的字符串，不区分大小写，只能以字母、数字和下划线开头；URI 正则表达式的取值范围为 4～253 个字符的字符串，区分大小写，只能以字母、数字和下划线开头。

text *string*：表示 URL 过滤规则使用文本对主机名和 URI 字段进行精确匹配。*string* 表示主机名或 URI 规则字符串，主机名规则的取值范围为 3～224 个字符的字符串，不区分大小写，主机名只能是字母、数字、下划线“_”、连接符“-”、冒号“：”、左方括号“[”、右方括号“]”和点号“.”，但 URI 无此限制；URI 规则的取值范围为 3～255 个字符的字符串，区分大小写。

【使用指导】

URL 过滤规则是指对用户 HTTP 报文中的 URL 进行匹配的原则，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。

【举例】

在 URL 过滤分类 news 中添加一条 URL 过滤规则，并使用字符串 sina.com 对主机名字段进行精确匹配。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] rule 10 host text sina.com
```

【相关命令】

- **url-filter category**

1.1.15 update schedule

update schedule 命令用来配置定期自动在线升级 URL 过滤特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

【缺省情况】

设备在每天 01:00:00 至 03:00:00 之间自动在线升级 URL 过滤特征库。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【参数】

daily：表示自动升级周期为每天。

weekly：表示以一周为周期，在指定的一天进行自动升级。

fri：表示星期五。

mon：表示星期一。

sat：表示星期六。

sun：表示星期日。

thu：表示星期四。

tue：表示星期二。

wed：表示星期三。

start-time *time*：指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00～23:59:59。

tingle *minutes*：指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置 URL 过滤特征库的定期自动在线升级时间为每周日 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
[Sysname] url-filter signature auto-update
[Sysname-url-filter-autoupdate] update schedule weekly sun start-time 20:30:00 tingle 10
```

【相关命令】

- **url-filter signatures auto-update**

1.1.16 url-filter apply policy

url-filter apply policy 命令用来在 DPI 应用 profile 中引用指定的 URL 过滤策略。

undo url-filter apply policy 命令用来删除引用的 URL 过滤策略。

【命令】

url-filter apply policy *policy-name*

undo url-filter apply policy

【缺省情况】

DPI 应用 profile 中未引用 URL 过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：URL 过滤策略名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

一个 DPI 应用 profile 下只能引用一个 URL 过滤策略。多次执行本命令，最后一次执行的命令生效。

【举例】

在名为 abc 的 DPI 应用 profile 下引用 URL 过滤策略 news。

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc]url-filter apply policy news
```

【相关命令】

- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **display app-profile**

- **display url-filter policy**

1.1.17 url-filter cache deploy-interval

url-filter cache deploy-interval 命令用来配置向应用层检测引擎下发缓存中规则的时间间隔。

undo url-filter cache deploy-interval 命令用来恢复缺省情况。

【命令】

url-filter cache deploy-interval *interval*

undo url-filter cache deploy-interval

【缺省情况】

向应用层检测引擎下发缓存中规则的时间间隔为 12 小时。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：指定向应用层检测引擎下发缓存中规则的时间间隔，取值范围为 1～65535，单位为小时。

【使用指导】

设备会根据配置的下发时间间隔将 URL 过滤缓存中的 URL 过滤规则定期下发到应用层检测引擎。配置的下发时间间隔不能太短，因为频繁下发 URL 过滤缓存规则可能会导致应用层检测引擎停止工作，从而会影响设备对其他 DPI 业务的处理。

【举例】

配置向应用层检测引擎下发缓存中规则的时间间隔为 24 小时。

```
<Sysname> system-view
[Sysname] url-filter cache deploy-interval 24
```

1.1.18 url-filter cache size

url-filter cache size 命令用来配置 URL 过滤缓存区可缓存记录的上限。

undo url-filter cache size 命令用来恢复缺省情况。

【命令】

url-filter cache size *cache-size*

undo url-filter cache size

【缺省情况】

URL 过滤缓存区可缓存记录的上限根据设备内存的实际大小由系统计算得出。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

cache-size：指定 URL 过滤缓存区可缓存记录的上限，取值范围为 1～65535。

【使用指导】

设备会把云端 URL 过滤分类服务器返回的查询结果缓存在 URL 过滤缓存中。后续符合此 URL 过滤规则的报文在流经设备时就会在本地匹配成功，而无需再进行云端查询。

配置的 URL 过滤缓存区可缓存记录的上限不能太大，因为大量 URL 过滤缓存规则的下发可能会导致应用层检测引擎停止工作，从而会影响设备对其他 DPI 业务的处理。

【举例】

配置 URL 过滤缓存区可缓存记录的上限为 20000。

```
<Sysname> system-view
[Sysname] url-filter cache size 20000
```

1.1.19 url-filter cache-time

url-filter cache-time 命令用来配置 URL 过滤缓存规则的最短保留时间。

undo url-filter cache-time 命令用来恢复缺省情况。

【命令】

url-filter cache-time *value*

undo url-filter cache-time

【缺省情况】

URL 过滤缓存规则的最短保留时间为 43200 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

value：指定 URL 过滤缓存规则的最短保留时间，取值范围为 1～4294967295，单位为秒。

【使用指导】

当从云端学习到的 URL 过滤规则在缓存中的保存时间达到指定的最短保留时间时，并不会被立刻删除，而是在如下情况下会被删除：

URL 过滤缓存已满后，如果从云端 URL 过滤分类服务器继续学习到了新的 URL 过滤规则，设备则从缓存中将保存时间超过最大缓存时间的最老 URL 过滤规则删除，然后将此新 URL 过滤规则添加到缓存中。

【举例】

配置 URL 过滤缓存规则的最短保留时间为 36000 秒。

```
<Sysname> system-view
[Sysname] url-filter cache-time 36000
```

1.1.20 url-filter category

url-filter category 命令用来创建 URL 过滤分类，并进入 URL 过滤分类视图。如果指定的 URL 过滤分类已经存在，则直接进入该 URL 过滤分类视图。

undo url-filter category 命令用来删除指定的 URL 过滤分类。

【命令】

url-filter category *category-name* [**severity** *severity-level*]

undo url-filter category *category-name*

【缺省情况】

只存在预定义的 URL 过滤分类，且分类名称以字符串 Pre-开头。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

category-name：表示 URL 过滤分类的名称，为 1～63 个字符的字符串，不区分大小写。不能以字符”Pre-“开头，因为 Pre-是预定义的 URL 过滤分类名称。

severity *severity-value*：表示 URL 过滤分类的严重级别属性。*severity-value* 为严重级别，取值范围为 1000～65535，创建 URL 过滤分类时必须配置此参数，数值越大表示严重级别越高，且不同的 URL 过滤分类的严重级别不能相同。

【使用指导】

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，其内容和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。

当报文匹配成功的 URL 过滤规则同属于多个 URL 过滤分类时，设备将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。

【举例】

创建一个名为 news 的 URL 过滤分类，指定其严重级别为 2000。

```
<Sysname> system-view
[Sysname] url-filter category news severity 2000
```

```
[Sysname-url-filter-category-news]
```

【相关命令】

- **display url-filter category**

1.1.21 url-filter category-server

url-filter category-server 命令用来配置云端 URL 过滤分类服务器的主机名。

undo url-filter category-server 命令用来删除指定的云端 URL 过滤分类服务器。

【命令】

url-filter category-server *host-name*

undo url-filter category-server *host-name*

【缺省情况】

不存在云端 URL 过滤分类服务器的主机名。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

host-name：表示云端 URL 过滤分类服务器主机名的名称，为 1～255 个字符的字符串，只能是字母、数字、下划线“_”、连接符“-”和点号“.”，不区分大小写。

【使用指导】

配置 URL 过滤分类云端查询功能时，需要确保设备能通过静态或动态域名解析方式获得云端 URL 过滤分类服务器的 IP 地址，并与之路由可达，否则设备进行 URL 过滤分类云端查询会失败。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”。

【举例】

指定 URL 过滤分类服务器的主机名为 urlservice.h3c.com。

```
<Sysname> system-view
[Sysname] url-filter category-server urlservice.h3c.com
```

1.1.22 url-filter copy category

url-filter copy category 命令用来复制 URL 过滤分类。

【命令】

url-filter copy category *old-name* [*new-name*] **severity** *severity-level*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name：原有分类名称。

new-name：新分类名称。如果不输入 *new-name*，则新创建 URL 过滤分类的名称默认为“*old-name_n*”，其中 n 为分类的复制次数，取值为整数形式，从 1 开始增加。

severity *severity-level*：表示 URL 过滤分类的严重级别。*severity-level* 为严重级别，取值范围为 1000～65535。数值越大表示严重级别越高，且不同的分类严重级别不能相同，如果相同，则复制失败。

【使用指导】

命令用来复制已存在的 URL 过滤分类，可以方便用户快速创建新的 URL 过滤分类。

【举例】

通过复制名称为 news 的 URL 过滤分类来创建 2 个新的 URL 过滤分类。

```
<Sysname> system-view
[Sysname] url-filter copy category news severity 1001
[Sysname-url-filter- category-news_1] quit
[Sysname] url-filter copy category news severity 1002
[Sysname-url-filter- category-news_2] quit
```

【相关命令】

- **url-filter category**

1.1.23 url-filter copy policy

url-filter copy policy 命令用来复制 URL 过滤策略。

【命令】

url-filter copy policy *old-name new-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name：原有策略名称。为 1～31 个字符的字符串，不区分大小写。

new-name：新策略名称。为 1～31 个字符的字符串，不区分大小写。

【使用指导】

命令用来复制已存在的 URL 过滤策略，可以方便用户快速创建新的 URL 过滤策略。

【举例】

通过复制名称为 news 的 URL 过滤策略来创建 2 个新的 URL 过滤策略。

```
<Sysname> system-view
[Sysname] url-filter copy policy news news1
[Sysname-url-filter-policy-news_1] quit
[Sysname] url-filter copy policy news new2
[Sysname-url-filter-policy-news_2] quit
```

【相关命令】

- **url-filter policy**

1.1.24 url-filter log directory root

url-filter log directory root 命令用来配置 URL 过滤仅对网站根目录下资源的访问进行日志记录。

undo url-filter log directory root 命令用来恢复缺省情况。

【命令】

url-filter log directory root

undo url-filter log directory root

【缺省情况】

URL 过滤对网站所有路径下资源的访问均进行日志记录。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

配置此命令后，**url-filter log except pre-defined** 和 **url-filter log except user-defined** 命令将失效。

【举例】

配置 URL 过滤仅对网站根目录下资源的访问进行日志记录。

```
<Sysname> system-view
[Sysname] url-filter log directory root
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log except pre-defined**
- **url-filter log except user-defined**

1.1.25 url-filter log enable

url-filter log enable 命令用来开启应用层检测引擎日志信息功能。

undo url-filter log enable 命令用来关闭应用层检测引擎日志信息功能。

【命令】

url-filter log enable

undo url-filter log enable

【缺省情况】

生成应用层检测引擎日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

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”。

【举例】

开启应用层检测引擎日志信息功能。

```
<Sysname> system-view
[Sysname] url-filter log enable
```

1.1.26 url-filter log except pre-defined

url-filter log except pre-defined 命令用来配置 URL 过滤对指定的预定义类型网页资源的访问不进行日志记录。

undo url-filter log except pre-defined 命令用来配置 URL 过滤对指定的预定义类型网页资源的访问进行日志记录。

【命令】

url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }

undo url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }

【缺省情况】

URL 过滤对所有预定义类型网页资源的访问不进行日志记录。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

css：表示网页资源类型为 css。

gif：表示网页资源类型为 gif。

ico：表示网页资源类型为 ico。

jpg：表示网页资源类型为 jpg。

js：表示网页资源类型为 js。

png：表示网页资源类型为 png。

swf：表示网页资源类型为 swf。

xml：表示网页资源类型为 xml。

【使用指导】

此命令生效的优先级低于 **url-filter log directory root** 命令，如果已经配置 **url-filter log directory root** 命令，则本配置不能生效。因此，如果要本配置生效，则需要执行 **undo url-filter log directory root** 命令。

可多次执行此命令，指定多种不记录访问日志的预定义网页资源类型。

【举例】

配置 URL 过滤对预定义 css 类型网页资源的访问不进行日志记录。

```
<Sysname> system-view
[Sysname] url-filter log except pre-defined css
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log directory root**
- **url-filter log except user-defined**

1.1.27 url-filter log except user-defined

url-filter log except user-defined 命令用来配置 URL 过滤对指定的自定义类型网页资源的访问不进行日志记录。

undo url-filter log except user-defined 命令用来配置 URL 过滤对指定的自定义类型网页资源的访问进行日志记录。

【命令】

url-filter log except user-defined *text*

undo url-filter log except user-defined [*text*]

【缺省情况】

未配置任何自定义类型网页资源。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：表示自定义网页资源类型，取值范围为 1～63 个字符的字符串，不区分大小写。

【使用指导】

此命令生效的优先级低于 **url-filter log directory root** 命令，如果已经配置 **url-filter log directory root** 命令，则本配置不能生效。因此，如果要本配置生效，则需要执行 **undo url-filter log directory root** 命令。

可多次执行此命令，指定多种不记录访问日志的自定义网页资源类型。

执行 **undo url-filter log except user-defined** 命令时，若未指定任何参数，则表示 URL 过滤对所有自定义类型网页资源的访问均进行日志记录。

【举例】

配置 URL 过滤对自定义 html 类型网页资源的访问不进行日志记录。

```
<Sysname> system-view
[Sysname] url-filter log except user-defined html
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log directory root**
- **url-filter log except pre-defined**

1.1.28 url-filter policy

url-filter policy 命令用来创建 URL 过滤策略，并进入 URL 过滤策略视图。如果指定的 URL 过滤策略已经存在，则直接进入 URL 过滤策略视图。

undo url-filter policy 命令用来删除指定的 URL 过滤策略。

【命令】

url-filter policy *policy-name*

undo url-filter policy *policy-name*

【缺省情况】

不存在 URL 过滤策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示 URL 过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

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 过滤策略中定义 URL 过滤策略的缺省动作。

只有在 DPI 应用 profile 中引用 URL 过滤策略后，设备的 URL 过滤功能才会生效。有关 DPI 应用 profile 的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

【举例】

创建一个名为 news 的 URL 过滤策略

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news]
```

1.1.29 url-filter signature auto-update

url-filter signature auto-update 命令用来开启定期自动在线升级 URL 过滤特征库功能，并进入自动升级配置视图。

undo url-filter signature auto-update 命令用来关闭定期自动在线升级 URL 过滤特征库功能。

【命令】

url-filter signature auto-update

undo url-filter signature auto-update

【缺省情况】

定期自动在线升级 URL 过滤特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问 H3C 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。

【举例】

开启定期自动在线升级 URL 过滤特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] url-filter signature auto-update
[Sysname-url-filter-autoupdate]
```

【相关命令】

- **update schedule**

1.1.30 url-filter signature auto-update-now

url-filter signature auto-update-now 命令用来立即自动在线升级 URL 过滤特征库。

【命令】

url-filter signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当管理员发现 H3C 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。

【举例】

立即自动在线升级 URL 过滤特征库版本。

```
<Sysname> system-view
[Sysname] url-filter signature auto-update-now
```

1.1.31 url-filter signature rollback

url-filter signature rollback 命令用来回滚 URL 过滤特征库版本。

【命令】

url-filter signature rollback { **factory** | **last** }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory：表示 URL 过滤特征库的出厂版本。

last：表示 URL 过滤特征库的上一版本。

【使用指导】

URL 过滤特征库回滚是指将当前的 URL 过滤特征库版本回滚到指定的 URL 过滤特征库版本。如果管理员发现设备对用户访问 Web 的 URL 过滤的误报率较高或出现异常情况，则可以对当前 URL 过滤特征库版本进行回滚。目前支持将设备中的 URL 过滤特征库版本回滚到出厂版本和上一版本。

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。

【举例】

配置 URL 过滤特征库回滚到上一版本。

```
<Sysname> system-view
[Sysname] url-filter signature rollback last
```

1.1.32 url-filter signature update

url-filter signature update 命令用来手动离线升级 URL 过滤特征库。

【命令】

url-filter signature update *file-path*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

file-path：指定特征库文件的路径，为 1～256 个字符的字符串。

【使用指导】

如果设备不能访问 H3C 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。特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。
- 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。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见表 1-5；FTP/TFTP 升级时参数 *file-path* 取值请参见表 1-6。

表1-5 本地升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件的存储位置与当前工作路径一致	*filename*	可以执行**pwd**命令查看当前工作路径 有关**pwd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	*path/ filename*	-

升级场景	参数 *file-path* 取值	说明
特征库文件的存储位置与当前工作路径不在相同存储介质上	*path/ filename*	需要先执行**cd**命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关**cd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-6 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件存储在开启FTP服务的远程服务器上	*ftp://username:password@server/filename*	*username*为登录FTP服务器的用户名，*password*为登录FTP服务器的密码，*server*为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启TFTP服务的远程服务器上	*tftp://server/filename*	*server*为TFTP服务器的IP地址或主机名

说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级 URL 过滤特征库，且采用 TFTP 方式，URL 过滤特征库文件的远程路径为 tftp://192.168.0.10/url-filter-1.0.2-en.dat。

```
<Sysname> system-view
[Sysname] url-filter signature update tftp://192.168.0.10/url-filter-1.0.2-en.dat
```

配置手动离线升级 URL 过滤特征库，且采用 FTP 方式，URL 过滤特征库文件的远程路径为 ftp://192.168.0.10/url-filter-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
[Sysname] url-filter signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/url-filter-1.0.2-en.dat
```

配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为 cfa0:/url-filter-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
[Sysname] url-filter signature update url-filter-1.0.23-en.dat
```

配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为 cfa0:/dpi/url-filter-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
```

```
[Sysname] url-filter signature update dpi/url-filter-1.0.23-en.dat
```

配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为 cfb0:/dpi/url-filter-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
<Sysname> system
[Sysname] url-filter signature update dpi/url-filter-1.0.23-en.dat
```

目　录

1 数据过滤

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：

型号	特性	描述
F1000-E-G2/F1000-A-G2/F1000-S-G2/F1000-C-G2	数据过滤	支持
F100-E-G2/F100-A-G2/F100-M-G2/F100-S-G2/F100-C-G2		• F100-M-G2/F100-S-G2/F100-C-G2：不支持 • F100-E-G2/F100-A-G2：支持
F1000-C-EI/F100-E-EI/F100-A-EI/F100-C-EI/F100-A-SI		• F100-C-EI：不支持 • F1000-C-EI/F100-E-EI/F100-A-EI/F100-A-SI：支持
F100-C-HI/F100-S-HI/F100-A-HI/F1000-C-HI		• F100-A-HI/F1000-C-HI：支持 • F100-C-HI/F100-S-HI：不支持
F1000-C8180/F1000-C8170/F1000-C8160/F1000-C8150/F1000-C8130/F1000-C8120		• F1000-C8180/F1000-C8170/F1000-C8160：支持 • F1000-C8150/F1000-C8130/F1000-C8120：不支持
F100-C80-WiNet/F100-C60-WiNet		不支持

1.1 数据过滤配置命令

1.1.1 action

action 命令用来配置数据过滤规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

action { **drop** | **permit** } [**logging**]

undo action

【缺省情况】

数据过滤规则的动作为丢弃。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

drop：表示丢弃报文。

permit：表示允许报文通过。

logging：表示生成日志信息。

【使用指导】

如果报文同时与多个规则匹配成功，则执行这些动作中优先级最高的动作，且动作优先级从高到低的顺序为：丢弃 > 允许，但是对于生成日志动作只要匹配成功的规则中存在就会执行。如果报文只与一个规则匹配成功，则执行此规则中的动作。

【举例】

创建一个名称为 def 的数据过滤策略。

```
<Sysname> system-view
[Sysname] data-filter policy def
```

在名称为 r1 的数据过滤规则中配置其动作为允许报文通过。

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] action permit
```

1.1.2 application

application 命令用来配置数据过滤规则的应用层协议类型。

undo application 命令用来删除指定的应用层协议类型。

【命令】

application { **all** | **type** { **ftp** | **http** | **smtp** } * }

undo application { **all** | **type** { **ftp** | **http** | **smtp** } * }

【缺省情况】

数据过滤规则中不存在应用层协议类型。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：表示数据过滤支持的所有应用层协议。

type：指定规则生效的协议类型。

ftp：表示 FTP 协议。

http：表示 HTTP 协议。

smtp：表示 SMTP 协议。

【使用指导】

通过配置此命令，可以根据业务应用所属的应用层协议类型来灵活控制对那些协议类型的报文进行数据过滤。

【举例】

创建一个名称为 def 的数据过滤策略。

```
<Sysname> system-view
[Sysname] data-filter policy def
```

在名称为 r1 的数据过滤规则中配置其应用层协议类型为 HTTP。

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] application type http
```

1.1.3 data-filter apply policy

data-filter apply policy 命令用来在 DPI 应用 profile 中引用指定的数据过滤策略。

undo data-filter apply policy 命令用来删除引用的数据过滤策略。

【命令】

data-filter apply policy *policy-name*

undo data-filter apply policy

【缺省情况】

DPI 应用 profile 中未引用数据过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：指定数据过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

通过在 DPI 应用 profile 中引用数据过滤策略，并将此 profile 应用于对象策略规则中来实现基于安全域间实例的 IP 报文过滤功能。

一个 DPI（Deep Packet Inspection，深度报文检测）应用 profile 下只能引用一个数据过滤策略。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 abc 的 DPI 应用 profile 下引用数据过滤策略 def。

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc] data-filter apply policy def
```

【相关命令】

- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **data-filter policy**

1.1.4 data-filter keyword-group

data-filter keyword-group 命令用来创建关键字组，并进入关键字组视图。如果指定的关键字组已经存在，则直接进入关键字组视图。

undo data-filter keyword-group 命令用来删除指定的关键字组。

【命令】

data-filter keyword-group *keywordgroup-name*

undo data-filter keyword-group *keywordgroup-name*

【缺省情况】

不存在关键字组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

keywordgroup-name：表示关键字组的名字，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

关键字组用来统一组织和管理设备中配置的数据过滤特征，一个关键字组中可以配置多个数据过滤特征，且它们之间是或的关系。

【举例】

创建一个名称为 kg1 的关键字组，并进入关键字组视图。

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-keygroup-kg1]
```

1.1.5 data-filter policy

data-filter policy 命令用来创建数据过滤策略，并进入数据过滤策略视图。如果数据过滤策略已经存在，则直接进入该数据过滤策略视图。

undo data-filter policy 命令用来删除指定的数据过滤策略。

【命令】

data-filter policy *policy-name*

undo data-filter policy *policy-name*

【缺省情况】

不存在数据过滤策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示数据过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

一个数据过滤策略中最多可创建 32 个数据过滤规则。

【举例】

创建一个名称为 def 的数据过滤策略，并进入该数据过滤策略视图。

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def]
```

【相关命令】

- **data-filter apply policy**

1.1.6 description (data-filter policy view)

description 命令用来配置数据过滤策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

不存在数据过滤策略的描述信息。

【视图】

数据过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

string：表示数据过滤策略的描述信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本数据过滤策略的作用。

【举例】

配置数据过滤策略 def 的描述信息为 The data filter。

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def] description The data filter
```

1.1.7 description (keyword-group view)

description 命令用来配置关键字组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

不存在关键字组的描述信息。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

string：关键字组的描述信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本关键字组的作用。

【举例】

配置关键字组 kg1 的描述信息为 The data filter keyword group。

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kgroup-kg1] description The data filter keyword group
```

1.1.8 direction

direction 命令用来配置数据过滤规则的匹配方向。

undo direction 命令用来恢复缺省情况。

【命令】

direction { **both** | **download** | **upload** }

undo direction

【缺省情况】

数据过滤规则的匹配方向为会话的上传方向。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

both：在会话的上传方向和下载方向都进行匹配。

download：在会话的下载方向进行匹配。

upload：在会话的上传方向进行匹配。

【使用指导】

通过配置此命令，可以根据报文传输的方向来灵活控制对那个方向的报文进行数据过滤。

【举例】

创建一个名称为 def 的数据过滤策略。

```
<Sysname> system-view
[Sysname] data-filter policy def
```

在名称为 r1 的数据过滤规则中配置其匹配方向为会话的下载方向。

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] direction download
```

1.1.9 keyword-group

keyword-group 命令用来在数据过滤规则中引用关键字组。

undo keyword-group 命令用来恢复缺省情况。

【命令】

keyword-group *keygroup-name*

undo keyword-group

【缺省情况】

数据过滤规则中未引用关键字组。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

keygroup-name：指定关键字组的名称，为 1～31 个字符的字符串，不区分大小写。指定的关键字组必须存在。

【使用指导】

在数据过滤规则中通过引用关键字组来对报文的应用层信息进行关键字匹配。

在同一个数据过滤规则视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

创建一个名称为 def 的数据过滤策略。

```
<Sysname> system-view
[Sysname] data-filter policy def
```

在名称为 r1 的数据过滤规则中引用关键字组 kg1。

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] keyword-group kg1
```

【相关命令】

- **data-filter keyword-group**

1.1.10 pattern

pattern 命令用来配置数据过滤特征。

undo pattern 命令用来删除指定的数据过滤特征。

【命令】

pattern *pattern-name* { **regex** | **text** } *pattern-string*

undo pattern *pattern-name*

【缺省情况】

关键字组中不存在数据过滤特征。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

pattern-name：表示数据过滤特征的名称，为 1～31 个字符的字符串，不区分大小写。

regex *pattern-string*：表示对应用层信息进行模糊匹配的正则表达式，为 3～245 个字符的字符串，区分大小写，支持所有可输入字符，且必须包含连续的 3 个非通配符。

text *pattern-string*：表示对应用层信息进行精确匹配的文本，为 3～245 个字符的字符串，支持所有可输入字符，区分大小写。

【使用指导】

一个数据过滤特征只能定义为一个正则表达式字符串或一个文本字符串。

一个关键字组中可以配置 32 个数据过滤特征，且它们之间是或的关系。

【举例】

在关键字组 kg1 中配置一条正则表达式，内容为(?i)^.*abc.*。

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kgroup-kg1] pattern 1 regex (?i)^.*abc.*
```

1.1.11 rule

rule 命令用来创建数据过滤规则，并进入数据过滤规则视图。如果数据过滤规则已经存在，则直接进入数据过滤规则视图。

undo rule 命令用来删除指定的数据过滤规则。

【命令】

rule *rule-name*

undo rule *rule-name*

【缺省情况】

不存在数据过滤规则。

【视图】

数据过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name：表示数据过滤规则的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

在数据过滤规则中可以配置匹配报文的一系列匹配项，比如规则匹配的方向、规则生效的协议类型、规则引用的关键字组和规则的动作。

【举例】

在名称为 def 的数据过滤策略下创建一个名称为 r1 的数据过滤规则，并进入数据过滤规则视图。

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1]
```

目　录

1 文件过滤

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：

型号	特性	描述
F1000-E-G2/F1000-A-G2/F1000-S-G2/F1000-C-G2	文件过滤	支持
F100-E-G2/F100-A-G2/F100-M-G2/F100-S-G2/F100-C-G2		• F100-M-G2/F100-S-G2/F100-C-G2：不支持 • F100-E-G2/F100-A-G2：支持
F1000-C-EI/F100-E-EI/F100-A-EI/F100-C-EI/F100-A-SI		• F100-C-EI：不支持 • F1000-C-EI/F100-E-EI/F100-A-EI/F100-A-SI：支持
F100-C-HI/F100-S-HI/F100-A-HI/F1000-C-HI		• F100-A-HI/F1000-C-HI：支持 • F100-C-HI/F100-S-HI：不支持
F1000-C8180/F1000-C8170/F1000-C8160/F1000-C8150/F1000-C8130/F1000-C8120		• F1000-C8180/F1000-C8170/F1000-C8160：支持 • F1000-C8150/F1000-C8130/F1000-C8120：不支持
F100-C80-WiNet/F100-C60-WiNet		不支持

1.1 文件过滤配置命令

1.1.1 action

action 命令用来配置文件过滤规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

action { **drop** | **permit** } [**logging**]

undo action

【缺省情况】

文件过滤规则的动作为丢弃。

【视图】

文件过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

drop：表示丢弃报文。

permit：表示允许报文通过。

logging：表示生成日志信息。

【使用指导】

如果文件的扩展名信息同时与多个规则匹配成功，则执行这些动作中优先级最高的动作，且动作优先级从高到低的顺序为：丢弃 > 允许，但是对于生成日志动作只要匹配成功的规则中存在就会执行。如果文件的扩展名信息只与一个规则匹配成功，则执行此规则中的动作。

【举例】

创建一个名称为 def 的文件过滤策略。

```
<Sysname> system-view
[Sysname] file-filter policy def
```

在名称为 ch1 的文件过滤规则中配置其动作为允许报文通过。

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] action permit
```

1.1.2 application

application 命令用来配置文件过滤规则的应用层协议类型。

undo application 命令用来删除指定的应用层协议类型。

【命令】

application { **all** | **type** { **ftp** | **http** | **smtp** } * }

undo application { **all** | **type** { **ftp** | **http** | **smtp** } * }

【缺省情况】

文件过滤规则中不存在应用层协议类型。

【视图】

文件过滤规则视图。

【缺省用户角色】

network-admin

context-admin

【参数】

all：表示文件过滤支持的所有应用层协议。

type：指定规则生效的协议类型。

ftp：表示 FTP 协议。

http：表示 HTTP 协议。

smtp：表示 SMTP 协议。

【使用指导】

通过配置此命令，可以根据文件传输所采用的应用层协议类型来灵活控制对哪些协议类型的报文进行文件过滤。

【举例】

创建一个名称为 def 的文件过滤策略。

```
<Sysname> system-view
[Sysname] file-filter policy def
```

在名称为 ch1 的文件过滤规则中配置其应用协议类型为 HTTP。

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] application type http
```

1.1.3 description (file-filter policy view)

description 命令用来配置文件过滤策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

不存在文件过滤策略的描述信息。

【视图】

文件过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

string：表示文件过滤策略的描述信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本文件过滤策略的作用，有利于后期维护。

【举例】

配置文件过滤策略 def 的描述信息为 The file filter。

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def] description The file filter
```

【相关命令】

- **file-filter policy**

1.1.4 description (filetype-group view)

description 命令用来配置文件类型组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

不存在文件类型组的描述信息。

【视图】

文件类型组视图

【缺省用户角色】

network-admin

context-admin

【参数】

string：文件类型组的描述信息，为 1～255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本文件类型组的作用，有利于后期维护。

【举例】

为文件类型组 abc 配置描述信息 def。

```
<Sysname> system-view
[Sysname] file-filter filetype-group abc
[Sysname-file-filter-fgroup-abc] description def
```

【相关命令】

- **file-filter filetype-group**

1.1.5 direction

direction 命令用来配置文件过滤规则的匹配方向。

undo direction 命令用来恢复缺省情况。

【命令】

direction { **both** | **download** | **upload** }

undo direction

【缺省情况】

文件过滤规则的匹配方向为上传方向。

【视图】

文件过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

both：在上传方向和下载方向都进行匹配。

download：在下载方向进行匹配。

upload：在上传方向进行匹配。

【使用指导】

通过配置此命令，可以根据报文传输的方向来灵活控制对那个方向的报文进行文件过滤。

对于 FTP 和 SMTP 协议上传方向和下载方向是指会话的上传和下载方向；对于 HTTP 协议上传方向是指 HTTP 协议 POST 类型的请求方法，下载方向是指 HTTP 协议 GET 类型的请求方法。

【举例】

创建一个名称为 def 的文件过滤策略。

```
<Sysname> system-view
[Sysname] file-filter policy def
```

在名称为 ch1 的文件过滤规则中配置其匹配方向为下载方向。

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] direction download
```

1.1.6 file-filter apply policy

file-filter apply policy 命令用来在 DPI 应用 profile 中引用文件过滤策略。

undo file-filter apply policy 命令用来取消 DPI 应用 profile 引用的文件过滤策略。

【命令】

file-filter apply policy *policy-name*

undo file-filter apply policy

【缺省情况】

DPI 应用 profile 中未引用文件过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：文件过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

通过在 DPI 应用 profile 中引用文件过滤策略，并将此 profile 应用于对象策略规则中来实现基于安全域间实例的文件过滤功能。

一个 DPI（Deep Packet Inspection，深度报文检测）应用 profile 下只能引用一个文件过滤策略。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 abc 的 DPI 应用 profile 下引用文件过滤策略 def。

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc] file-filter apply policy def
```

【相关命令】

- **app-profile**
- **file-filter policy**

1.1.7 file-filter filetype-group

file-filter filetype-group 命令用来创建文件类型组，并进入文件类型组视图。如果指定的文件类型组已经存在，则直接进入文件类型组视图。

undo file-filter filetype-group 命令用来删除指定的文件类型组。

【命令】

file-filter filetype-group *group-name*

undo file-filter filetype-group *group-name*

【缺省情况】

不存在文件类型组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name：表示文件类型组的名字，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

文件类型组用来统一组织和管理设备中配置的文件过滤特征。一个文件类型组中可以配置多个文件过滤特征，且它们之间是或的关系。

【举例】

创建一个名称为 fg1 的文件类型组，并进入文件类型组视图。

```
<Sysname> system-view
[Sysname] file-filter filetype-group fg1
```

```
[Sysname-file-filter-fgroup-fg1]
```

1.1.8 file-filter policy

file-filter policy 命令用来创建文件过滤策略，并进入文件过滤策略视图。如果指定的文件过滤策略已经存在，则直接进入文件过滤策略视图。

undo file-filter policy 命令用来删除指定的文件过滤策略。

【命令】

file-filter policy *policy-name*

undo file-filter policy *policy-name*

【缺省情况】

不存在文件过滤策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：文件过滤策略的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

一个文件过滤策略中最多可以定义 32 个文件过滤规则。

【举例】

创建一个名称为 def 的文件过滤策略，并进入该文件过滤策略视图。

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def]
```

【相关命令】

- **file-filter apply policy**

1.1.9 filetype-group

filetype-group 命令用来在文件过滤规则中引用文件类型组。

undo filetype-group 命令用来恢复缺省情况。

【命令】

filetype-group *group-name*

undo filetype-group

【缺省情况】

文件过滤规则中未引用文件类型组。

【视图】

文件过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name：指定文件类型组的名称，为 1～31 个字符的字符串，不区分大小写。指定的文件类型组必须存在。

【使用指导】

在文件过滤规则中通过引用文件类型组来对文件的扩展名信息进行精确匹配。

在同一个文件过滤规则视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

创建一个名称为 def 的文件过滤策略。

```
<Sysname> system-view
[Sysname] file-filter policy def
```

在名称为 ch1 的文件过滤规则中引用文件类型组 fg1。

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] filetype-group fg1
```

【相关命令】

- **file-filter filetype-group**

1.1.10 pattern

pattern 命令用来配置文件过滤特征。

undo pattern 命令用来删除指定的文件过滤特征。

【命令】

pattern *pattern-name* **text** *pattern-string*

undo pattern *pattern-name*

【缺省情况】

文件类型组中不存在文件过滤特征。

【视图】

文件类型组视图

【缺省用户角色】

network-admin

context-admin

【参数】

pattern-name：表示文件过滤特征的名字，为 1～31 个字符的字符串，不区分大小写。

text *pattern-string*：表示对文件的扩展名信息进行精确匹配的文本，*pattern-string* 是文本内容，为 1～8 个字符的字符串，区分大小写。

【使用指导】

文件过滤特征是设备执行文件过滤功能时系统需要对文件的扩展名信息进行识别的内容。

一个文件类型组中可以配置 32 个文件过滤特征，且它们之间是或的关系。

【举例】

在文件类型组 fg1 中配置文件过滤特征为 doc。

```
<Sysname> system-view
[Sysname] file-filter filetype-group fg1
[Sysname-file-filter-fgroup-fg1] pattern 1 text doc
```

1.1.11 rule

rule 命令用来创建文件过滤规则，并进入文件过滤规则视图。如果指定的文件过滤视图已经存在，则直接进入文件过滤视图。

undo rule 命令用来删除指定的文件过滤规则。

【命令】

rule *rule-name*

undo rule *rule-name*

【缺省情况】

不存在文件过滤规则。

【视图】

文件过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name：文件过滤规则的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

在文件过滤规则中可以配置匹配报文的一系列匹配项，比如规则匹配的方向、规则生效的协议类型、规则引用的文件类型组和规则的动作。

只有文件属性（包括文件的应用类型、传输方向和扩展名）成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

一个文件过滤策略中最多可以定义 32 个文件过滤规则。

【举例】

在名称为 def 的文件过滤策略下创建一个名称为 ch1 的文件过滤规则，并进入文件过滤规则视图。

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def]rule ch1
```

```
[Sysname-file-filter-policy-def-rule-ch1]
```

目 录

1 防病毒

1.1 防病毒配置命令

1.1.1 anti-virus apply policy

anti-virus apply policy 命令用来在 DPI 应用 profile 中引用防病毒策略。

undo anti-virus apply policy 命令用来删除引用的防病毒策略。

【命令】

anti-virus apply policy *policy-name* **mode** { **alert** | **protect** }

undo anti-virus apply policy

【缺省情况】

DPI 应用 profile 中未引用防病毒策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示防病毒策略名称，为 1～63 个字符的字符串，不区分大小写。

mode：表示防病毒策略的模式。

alert：告警模式，表示报文匹配上该防病毒策略中的特征后，仅可以生成日志，但其他动作均不生效。

protect：保护模式，表示报文匹配上该防病毒策略中的特征后，设备按照特征的动作对该报文进行处理。

【使用指导】

一个 DPI 应用 profile 视图下只能引用一个防病毒策略。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 sec 的 DPI 应用 profile 下引用防病毒策略 abc。

```
<Sysname> system-view
[Sysname] app-profile sec
[Sysname-app-profile-sec] anti-virus apply policy abc mode protect
```

1.1.2 anti-virus policy

anti-virus policy 命令用来创建防病毒策略，并进入防病毒策略视图。如果指定的防病毒策略已经存在，则直接进入防病毒策略视图。

undo anti-virus policy 命令用来删除指定的防病毒策略。

【命令】

anti-virus policy *policy-name*

undo anti-virus policy *policy-name*

【缺省情况】

存在一个缺省防病毒策略，名称为 default。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示防病毒策略的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

缺省防病毒策略和自定义防病毒策略都使用当前系统中的所有病毒特征。

缺省防病毒策略不能被修改和删除。

【举例】

创建一个名称为 abc 的防病毒策略，并进入防病毒策略视图。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc]
```

1.1.3 anti-virus parameter-profile

anti-virus parameter-profile 命令用来引用应用层检测引擎动作参数 profile。

undo anti-virus parameter-profile 命令用来取消引用应用层检测引擎动作参数 profile。

【命令】

anti-virus { **email** | **logging** | **redirect** } **parameter-profile** *profile-name*

undo anti-virus { **email** | **logging** | **redirect** } **parameter-profile**

【缺省情况】

防病毒未引用应用层检测引擎动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

email：表示引用应用层检测引擎邮件动作参数 profile。

logging：表示引用应用层检测引擎日志动作参数 profile。

redirect：表示引用应用层检测引擎重定向动作参数 profile。

parameter-profile *parameter-name*：指定防病毒动作引用的应用层检测引擎动作参数 profile。*parameter-name* 表示动作参数 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

防病毒动作的具体执行参数（例如，邮件服务器的地址、输出日志的方式和对报文重定向的 URL）由应用层检测引擎各动作参数 profile 来定义，可通过引用各动作参数 proflle 为防病毒动作提供执行参数。应用层检测引擎动作参数 proflle 的具体配置请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

如果防病毒没有引用应用层检测引擎动作参数 profile，或者引用的动作参数 profile 不存在，则使用系统中各动作参数的缺省值。

【举例】

创建名称为 av1 的应用层检测引擎邮件动作参数 profile，配置登录邮件服务器的明文密码为 abc123。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile av1
[Sysname-inspect-email-av1] password simple abc123
[Sysname-inspect-logging-av1] quit
```

引用名称为 av1 的应用层检查引擎邮件动作参数 profile。

```
[Sysname] anti-virus email parameter-profile av1
```

【相关命令】

- **inspect email parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect logging parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect redirect parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）

1.1.4 anti-virus signature auto-update

anti-virus signature auto-update 命令用来开启定期自动在线升级病毒特征库功能，并进入自动升级配置视图。

undo anti-virus signature auto-update 命令用来关闭定期自动在线升级病毒特征库功能。

【命令】

anti-virus signature auto-update

undo anti-virus signature auto-update

【缺省情况】

定期自动在线升级病毒特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问 H3C 官方网站，可以采用定期自动在线升级方式来对设备上的病毒特征库进行升级。

【举例】

开启定期自动在线升级病毒特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update
[Sysname-anti-virus-autoupdate]
```

【相关命令】

- **update schedule**

1.1.5 anti-virus signature auto-update-now

anti-virus signature auto-update-now 命令用来立即自动在线升级病毒特征库。

【命令】

anti-virus signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行此命令后，将立即自动升级设备上的病毒特征库，且会备份当前的病毒特征库文件。此命令的生效与否，与是否开启了定期自动升级病毒特征库功能无关。

当管理员发现 H3C 官方网站上的特征库服务专区中的病毒特征库有更新时，可以选择立即自动在线升级方式来及时升级病毒特征库版本。

【举例】

立即自动在线升级病毒特征库版本。

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update-now
```

1.1.6 anti-virus signature rollback

anti-virus signature rollback 命令用来回滚病毒特征库。

【命令】

anti-virus signature rollback { **factory** | **last** }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory：表示病毒特征库的出厂版本。

last：表示病毒特征库的上一版本。

【使用指导】

如果管理员发现设备当前病毒特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前病毒特征库版本进行回滚。目前支持将设备中的病毒过滤特征库版本回滚到出厂版本和上一版本。

病毒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，当前病毒特征库版本是 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。

【举例】

配置病毒特征库回滚到上一版本。

```
<Sysname> system-view
[Sysname] anti-virus signature rollback last
```

1.1.7 anti-virus signature update

anti-virus signature update 命令用来手动离线升级病毒特征库。

【命令】

anti-virus signature update *file-path*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

file-path：指定病毒特征库文件的路径，为 1～255 个字符的字符串。

【使用指导】

如果设备不能访问 H3C 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病毒特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的病毒特征库版本。特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

- 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，并升级系统上的病毒特征库版本。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见表 1-1；FTP/TFTP 升级时参数 *file-path* 取值请参见表 1-2。

表1-1 本地升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件的存储位置与当前工作路径一致	*filename*	可以执行**pwd**命令查看当前工作路径 有关**pwd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	*path/ filename*	-
特征库文件的存储位置与当前工作路径不在相同存储介质上	*path/ filename*	需要先执行**cd**命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关**cd**命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-2 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 *file-path* 取值	说明
特征库文件存储在开启FTP服务的远程服务器上	*ftp://username:password@server/filename*	*username*为登录FTP服务器的用户名，*password*为登录FTP服务器的密码，*server*为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启TFTP服务的远程服务器上	*tftp://server/filename*	*server*为TFTP服务器的IP地址或主机名

说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级病毒特征库，且采用 TFTP 方式，病毒特征库文件的远程路径为 tftp://192.168.0.10/av-1.0.2-en.dat。

```
<Sysname> system-view
[Sysname] anti-virus signature update tftp://192.168.0.10/av-1.0.2-en.dat
```

配置手动离线升级病毒特征库，且采用 FTP 方式，病毒特征库文件的远程路径为 ftp://192.168.0.10/av-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
[Sysname] anti-virus signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/av-1.0.2-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfa0:/av-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
[Sysname] anti-virus signature update av-1.0.23-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfa0:/dpi/av-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system
[Sysname] anti-virus signature update dpi/av-1.0.23-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfb0:/dpi/av-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
<Sysname> system
[Sysname] anti-virus signature update dpi/av-1.0.23-en.dat
```

1.1.8 description

description 命令用来配置防病毒策略描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

不存在防病毒策略描述信息。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：防病毒策略的描述信息，为 1～255 个字符的字符串，可以包含空格，区分大小写。

【使用指导】

描述信息便于管理员快速理解和识别本防病毒策略的作用，有利于后期维护。

【举例】

配置防病毒策略 abc 的描述信息为"RD Department anti-virus policy"。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
```

```
[Sysname-anti-virus-policy-abc] description "RD Department anti-virus policy"
```

1.1.9 display anti-virus signature

display anti-virus signature 命令用来显示病毒特征信息。

【命令】

display anti-virus signature [[*signature-id*] [**severity** { **critical** | **high** | **low** | **medium** }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

signature-id：表示病毒特征的 ID 号，取值范围为 1～4294967294。

severity：指定病毒特征攻击的严重级别。

critical：表示严重级别最高。

high：表示严重级别比较高。

low：表示严重级别最低。

medium：表示严重级别中等。

【使用指导】

可以通过本命令来了解病毒特征的严重级别，便于更加合理的使用 **signature severity enable** 来使相应级别的病毒特征生效。

【举例】

显示所有病毒特征。

```
<Sysname> display anti-virus signature
 Total count       :9206      failed:0

Sig-ID    Severity Virus Name
1         LOW      Hoax.Win32.ArchSMS.pxm
2         LOW      Trojan.Win32.Inject.acwr
3         LOW      Virus.Win32.Alman.b
4         LOW      Hoax.Win32.ArchSMS.ovq
5         LOW      Hoax.Win32.ArchSMS.owa
6         LOW      Trojan-PSW.Win32.Dybalom.dhc
7         LOW      Trojan.Win32.Llac.has
8         LOW      HackTool.Win32.Kiser.tk
9         LOW      Trojan-Dropper.Win32.Pincher.hp
10        LOW      Trojan.Win32.Agent.cccr
11        LOW      Trojan.Win32.VkHost.lz
```

```
12          LOW       Backdoor.MSIL.Agent.ju
13          LOW       Backdoor.Win32.Bifrose.fqv
14          LOW       Backdoor.Win32.Bifrose.fwg
15          LOW       Backdoor.Win32.Bifrose.uw
---- More ----
```

表1-3 display anti-virus signature 命令显示信息描述表

字段	描述
Total count	病毒特征的总数
Failed	从病毒特征库下发应用层检测引擎失败病毒特征的个数
Sig-ID	病毒特征的编号
Severity	病毒特征的攻击严重级别属性，从低到高分为四级：Low、Medium、High、Critical
Virus Name	病毒特征的名称

1.1.10 display anti-virus signature information

display anti-virus signature information 命令用来显示病毒特征库信息。

【命令】

display anti-virus signature information

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示病毒特征库信息。

```
<Sysname> display anti-virus signature information
Anti-Virus signature library information:
Type       SigVersion         ReleaseTime               Size
Current    1.0.9              Wed Apr 22 09:51:13 2015  976432
Last       -                  -                         -
Factory    1.0.8              Fri Feb 06 05:48:40 2015  273248
```

表1-4 display anti-virus signature information 命令显示信息描述表

字段	描述
Type	病毒特征库版本，包括如下取值： • Current：当前版本 • Last：上一版本 • Factory：出厂版本
SigVersion	病毒特征库版本号
ReleaseTime	病毒特征库发布时间
Size	病毒特征库大小，单位是Bytes

1.1.11 display anti-virus statistics

display anti-virus statistics 命令用来显示防病毒统计信息。

【命令】

display anti-virus statistics [**policy** *policy-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

policy *policy-name*：表示防病毒策略名称，为 1～63 个字符的字符串，不区分大小写。若不指定此参数，则显示所有防病毒策略的统计信息。

slot *slot-number*：显示指定成员设备上的防病毒统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上的防病毒统计信息。

【举例】

显示防病毒策略 aa 的统计信息。

```
<Sysname> display anti-virus statistics policy aa
Slot 1:
Total Block:    0
Total Redirect: 0
Total Alert:    0
Type           http      ftp       smtp      pop3      imap
Block           0         0         0         0         0
Redirect        0         0         0         0         0
Alert+Permit    0         0         0         0         0
```

表1-5 display anti-virus statisic 命令显示信息描述表

字段	描述
Total Block	执行阻断动作的总数
Total Redirect	执行重定向动作的总数
Total Alert	执行告警动作的总数
Type	动作类型，包括如下取值： • Block：表示阻断报文并生成日志。 • Redirect：表示将 HTTP 连接重定向到指定的 URL 并生成日志。 • Alert+Permit：表示仅对报文进行告警，即允许报文通过并生成日志。
http	对HTTP协议类型数据处理的动作计数
ftp	对FTP协议类型数据处理的动作计数
smtp	对SMTP协议类型数据处理的动作计数
pop3	对POP3协议类型数据处理的动作计数
imap	对IMAP协议类型数据处理的动作计数

1.1.12 exception application

exception application 命令用来配置应用例外并为其指定处理动作。

undo exception application 命令用来删除指定的或所有的应用例外。

【命令】

exception application *application-name* **action** { **alert** | **block** | **permit** }

undo exception application { *application-name* | **all** }

【缺省情况】

不存在应用例外。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

application-name：例外应用的名称。

action：指定例外应用的动作。

all：表示所有的应用例外。

alert：表示仅对病毒报文进行告警，即允许其通过并生成病毒日志。

block：表示阻断病毒报文并生成病毒日志。

permit：表示允许病毒报文通过。

【使用指导】

缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理。当需要对某应用层协议上承载的某一具体应用采取不同的动作时，可以将此应用设置为应用例外。例如，对 HTTP 协议进行允许通过处理，但是需要对 HTTP 协议上承载的游戏类应用采取阻断动作，这时就可以把所有游戏类的应用设置为应用例外。

【举例】

配置 163Email 应用为应用例外并为其指定处理动作为告警。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception application 163Email action alert
```

1.1.13 exception signature

exception signature 命令用来配置病毒例外。

undo exception signature 命令用来删除指定的或所有的病毒例外。

【命令】

exception signature *signature-id*

undo exception signature { *signature-id* | **all** }

【缺省情况】

不存在病毒例外。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

signature-id：表示病毒特征的 ID 号，取值范围为 1～4294967294。

all：表示所有的病毒例外。

【使用指导】

如果发现某类检测出病毒的报文被误报时，可以通过执行此命令把该报文对应的病毒特征设置为病毒例外。当后续再有检测出包含此病毒特征的报文通过时，设备将对其执行允许动作。

【举例】

配置 ID 为 95 的病毒特征为病毒例外。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception signature 95
```

【相关命令】

- **display anti-virus signature**

1.1.14 inspect

inspect 命令用来配置病毒检测的应用层协议类型。

undo inspect 命令用来取消对指定协议的报文进行病毒检测。

【命令】

inspect { **ftp** | **http** | **imap** | **pop3** | **smtp** } [**direction** { **both** | **download** | **upload** }] [**action** { **alert** | **block** | **redirect** }]

undo inspect { **ftp** | **http** | **imap** | **pop3** | **smtp** }

【缺省情况】

设备对 FTP、HTTP 和 IMAP 协议上传和下载方向传输的报文均进行病毒检测，对 POP3 协议下载方向传输的报文进行病毒检测，对 SMTP 协议上传方向传输的报文进行病毒检测。设备对 FTP、HTTP 协议报文的动作为阻断，对 IMAP、SMTP 和 POP3 协议报文的动作为告警。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ftp：表示 FTP 协议。

http：表示 HTTP 协议。

imap：表示 IMAP 协议。

pop3：表示 POP3 协议。

smtp：表示 SMTP 协议。

direction：表示对指定方向上的报文进行病毒检测。

both：表示会话的上传和下载方向。

download：表示会话的下载方向。

upload：表示会话的上传方向。

action：指定对报文的处理动作。

alert：表示仅对病毒报文进行告警，即允许其通过并生成病毒日志。

block：表示阻断病毒报文并生成病毒日志。

redirect：表示将携带病毒的 HTTP 连接重定向到指定的 URL 并生成病毒日志。

【使用指导】

配置此命令后，设备可根据报文的应用层协议类型和传输方向来对其进行病毒检测，如果检测到病毒，则对此报文执行指定的动作。

因为防病毒模块所支持协议的连接请求均由客户端发起，为了使连接可以成功建立并能对此连接上的报文进行病毒检测，需要管理员在配置安全域间实例时确保客户端所在的安全域为源安全域、服务器所在的安全域为目的安全域。

因为 POP3 协议只有下载方向，SMTP 协议只支持上传方向，所以对这两种协议类型不支持配置方向属性。

IMAP 协议只支持告警动作。

【举例】

配置对基于 HTTP 协议且是下载方向上的报文进行检测病毒，动作为告警。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] inspect http direction download action alert
```

配置不对基于 FTP 协议的报文进行病毒检测。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] undo inspect ftp
```

1.1.15 signature severity enable

signature severity enable 命令用来配置有效病毒特征的最低严重级别。

undo signature severity enable 命令用来恢复缺省情况。

【命令】

signature severity { **critical** | **high** | **medium** } **enable**

undo signature severity enable

【缺省情况】

所有严重级别的病毒特征都处于生效状态。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

critical：表示严重级别最高。

high：表示严重级别比较高。

medium：表示严重级别中等。

【使用指导】

在仅需要对某类及其以上严重级别病毒进行防御的应用需求中，可通过配置此功能来实现此种应用需求。配置此功能后防病毒策略中只有指定的及其以上严重级别的病毒特征会生效。

【举例】

配置仅使 High 及其以上严重级别的病毒特征生效。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] signature severity high enable
```

1.1.16 update schedule

update schedule 命令用来配置定期自动在线升级病毒特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

【缺省情况】

设备在每天 02:01:00 至 04:01:00 之间自动在线升级病毒特征库。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【参数】

daily：表示升级周期为每天。

weekly：表示以一周为周期，在指定一天进行自动升级。

fri：表示星期五。

mon：表示星期一。

sat：表示星期六。

sun：表示星期日。

thu：表示星期四。

tue：表示星期二。

wed：表示星期三。

start-time *time*：指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

tingle *minutes*：指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置病毒特征库的定期自动在线升级时间为每周一 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update
[Sysname-anti-virus-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

【相关命令】

- **anti-virus signature auto-update**