目 录

1 IPS

1.1 IPS配置命令

1.1.1 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

【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
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 • Redirect：表示重定向报文的动作，把符合特征的报文重定向到指定的Web页面上 • Reset：表示发送 TCP 的 reset 报文使 TCP 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

【相关命令】

- **ips policy**

1.1.2 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

【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
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

1.1.3 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

【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，取值范围为 1～4294967295。

【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1-3 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 • Redirect：表示重定向报文的动作，把符合特征的报文重定向到指定的Web页面上 • Reset：表示发送 TCP 的 reset 报文使 TCP 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

字段	描述
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

1.1.4 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

【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1-4 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

字段	描述
ReleaseTime	IPS特征库发布时间
Size	IPS特征库文件大小，单位是Bytes

1.1.5 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

【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**

1.1.6 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

【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）

1.1.7 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

【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]
```

1.1.8 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

【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**

1.1.9 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

【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
```

1.1.10 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

【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。

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 1-5；采用FTP/TFTP方式时参数 *file-path*取值请参见表 1-6。

表1-5 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1-6 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”
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。

【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
```

1.1.11 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

【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
```

1.1.12 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

【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。
- 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。

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。（集中式设备-IRF 模式）

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 1-7；FTP/TFTP升级时参数 *file-path*取值请参见表 1-8。

表1-7 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1-8 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
```

1.1.13 object-dir

object-dir命令用来通过配置方向选择IPS策略所保护的对象。

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 策略保护所有方向上的对象。

【视图】

IPS 策略视图

【缺省用户角色】

network-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。

【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
```

1.1.14 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

【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**

1.1.15 protect-target

protect-target命令用来配置IPS策略保护对象的筛选条件。

undo protect-target命令用来删除IPS策略保护对象的筛选条件。

【命令】

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

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

【缺省情况】

IPS 策略中没有配置保护对象的筛选条件，IPS 策略保护所有对象。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

【参数】

all：表示保护所有对象。

target：表示对象分类。

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

【使用指导】

可通过配置保护对象来筛选此IPS策略中需要匹配的IPS特征，从而实现保护某对象的功能，未被选中的对象不受此IPS策略的保护。在IPS策略视图下执行 **display this**命令可查看此策略保护的所有对象。

可多次执行本命令，为 IPS 策略配置多个保护对象。

【举例】

在名称为 test 的 IPS 策略中，配置策略保护的子对象为 WebServer 对象分类中的 WebLogic。

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

1.1.16 severity-level

severity-level命令用来通过配置严重级别选择IPS策略所保护的对象。

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 策略保护所有严重级别的对象。

【视图】

IPS 策略视图

【缺省用户角色】

network-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。

【举例】

在名称为 test 的 IPS 策略中仅保护严重级别为 critical 和 medium 的对象。

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

1.1.17 signature override

signature override命令用来修改IPS特征的状态和动作。

undo signature override命令用来恢复指定IPS特征的缺省状态和动作。

【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

【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：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：表示丢弃报文的动作。

permit：表示允许报文通过的动作。

redirect：表示重定向报文的动作，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报文使TCP连接断开。

capture：表示捕获报文的动作。

logging：表示生成报文日志的动作。

【使用指导】

管理员可以根据实际的网络需求，通过配置 IPS 策略修改此 IPS 策略中已有 IPS 特征的动作属性和生效状态属性，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。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。

经过设备的报文与某个 IPS 特征匹配成功后，设备将根据此 IPS 特征的动作对该报文进行处理。如果报文未与任何 IPS 特征匹配成功，则设备直接允许此报文通过。

如果报文同时与多个 IPS 特征匹配成功，则根据这些动作中优先级最高的动作对此报文进行处理。但是，对于源阻断、生成日志和捕获三个动作只要匹配成功的特征中存在就会执行。动作优先级从高到低的顺序为：重置 > 重定向 > (源阻断/丢弃) > 允许，其中源阻断与丢弃的优先级相同。

【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 global enable**（安全命令参考/攻击检测与防范）
- **ips parameter-profile**
- **ips policy**

1.1.18 signature override all

signature override all命令用来配置IPS策略动作。

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 策略执行特征中定义的动作。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin

【参数】

block-source：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：表示丢弃报文的动作。

permit：表示允许报文通过的动作。

redirect：表示重定向报文的动作，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报文使TCP连接断开。

capture：表示捕获报文的动作。

logging：表示生成报文日志的动作。

【使用指导】

若为某 IPS 策略配置了动作，则设备将根据 IPS 策略中配置的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 IPS 策略中特征的预定义动作对与此特征匹配成功的报文进行处理。当 IPS 特征中的动作被修改后，无论是否 IPS 策略中配置了动作，设备都将根据 IPS 特征中自定义的动作对与此特征匹配成功的报文进行处理。

【举例】

配置名称为 text 的 IPS 策略的动作为丢弃，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 global enable**（安全命令参考/攻击检测与防范）
- **ips parameter-profile**

1.1.19 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 02:01:00 至 04:01:00 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

【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**