H3C WA 系列无线接入点

WLAN 安全命令参考

新华三技术有限公司
http://www.h3c.com

资料版本：6W100-20180921
产品版本：R2414

前 言

本命令参考主要介绍 H3C WA 系列无线接入点 WLAN 用户安全命令以及 WIPS 命令等内容。

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 WLAN用户安全

1.1 WLAN用户安全配置命令

1.1.1 akm mode

akm mode 命令用来配置身份认证与密钥管理的模式。

undo akm mode 命令用来恢复缺省情况。

【命令】

akm mode { **dot1x** | **private-psk** | **psk** }

undo akm mode

【缺省情况】

未配置身份认证与密钥管理。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

dot1x：表示身份认证与密钥管理的模式是 802.1X 模式。

private-psk：表示身份认证与密钥管理的模式是 Private-PSK 模式。

psk：表示身份认证与密钥管理的模式是 PSK 模式。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置，并且只能配置一种模式。

当 WLAN 网络采用 RSNA 安全机制时，必须配置身份认证与密钥管理。

每一种身份认证模式都有互相依赖的用户认证方式：

- 802.1X 模式和 802.1X 用户认证模式相互依赖，必须同时配置。有关 802.1X 的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- Private-PSK 模式和 MAC 地址认证模式相互依赖，必须同时配置，有关 MAC 地址认证的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- PSK 模式和 MAC 地址认证模式或 Bypass 用户认证模式相互依赖，必须同时配置。有关 MAC 地址认证和 Bypass 认证的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。

【举例】

配置身份认证与密钥管理模式为 PSK 模式。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] akm mode psk
```

【相关命令】

- **cipher-suite**
- **security-ie**

1.1.2 cipher-suite

cipher-suite 命令用来配置在帧加密时使用的加密套件。

undo cipher-suite 命令用来取消在帧加密时使用指定的加密套件。

【命令】

cipher-suite { ccmp | tkip | wep40 | wep104 | wep128 }

undo cipher-suite { ccmp | tkip | wep40 | wep104 | wep128 }

【缺省情况】

未配置加密套件。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

ccmp：AES-CCMP 加密套件。

tkip：TKIP 加密套件。

wep40：WEP40 加密套件。

wep104：WEP104 加密套件。

wep128：WEP128 加密套件。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

如果配置了安全 IE，则必须配置 TKIP 或者 CCMP 加密套件中的一种。当 WLAN 网络采用 RSNA 安全机制时，必须配置加密套件。

WEP 加密套件只能配置 WEP40/WEP104/WEP128 其中的一种，且需要配置与加密套件种类相对应的 WEP 密钥及 WEP 密钥 ID。

WEP128 和 CCMP 或 TKIP 不能同时配置。

【举例】

配置在帧加密时使用 TKIP 加密套件。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] cipher-suite tkip
```

【相关命令】

- **security-ie**
- **wep key**

- **wep key-id**

1.1.3 gtk-rekey client-offline enable

gtk-rekey client-offline enable 命令用来开启客户端离线更新 GTK 功能。

undo gtk-rekey client-offline enable 命令用来关闭客户端离线更新 GTK 功能。

【命令】

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

【缺省情况】

客户端离线更新 GTK 功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

只有开启了更新 GTK 功能，客户端离线更新 GTK 的功能才能生效。

【举例】

开启客户端离线更新 GTK 功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey client-offline enable
```

【相关命令】

- **gtk-rekey enable**

1.1.4 gtk-rekey enable

gtk-rekey enable 命令用来开启更新 GTK 功能。

undo gtk-rekey enable 命令用来关闭更新 GTK 功能。

【命令】

gtk-rekey enable

undo gtk-rekey enable

【缺省情况】

更新 GTK 功能处于开启状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【举例】

开启更新 GTK 功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey enable
```

1.1.5 gtk-rekey method

gtk-rekey method 命令用来配置 GTK 更新方法。

undo gtk-rekey method 命令用来恢复缺省情况。

【命令】

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

【缺省情况】

GTK 更新采用基于时间的方法，时间间隔为 86400 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

packet-based：表示基于数据包的更新方法。

packet：指定传输的数据包（包括组播和广播）的数目，在传送指定数目的数据包（包括组播和广播）后更新 GTK，取值范围为 5000～4294967295，缺省值为 10000000。

time-based：表示基于时间的 GTK 更新方法。

time：指定 GTK 密钥更新的周期。取值范围为 180～604800，单位为秒，缺省值为 86400 秒。

【使用指导】

只有开启了 GTK 更新功能，GTK 更新方法才能生效。

使用该命令配置 GTK 密钥更新方法，多次执行本命令，最后一次执行的命令生效。例如，如果先配置了基于数据包的方法，然后又配置了基于时间的方法，则最后生效的是基于时间的方法。

若该命令在无线服务模板处于开启状态下配置，则分为以下几种情况：

- 基于时间的 GTK 的更新方式不改变，只改变时间值，则在原有定时器超时之后，新的定时器才可以生效；
- 基于报文数的 GTK 更新方式不改变，只改变报文数值，则该新的配置立即生效；
- 更新方式由基于时间更新改为基于报文数更新，则删除 GTK 更新定时器，在组播或广播报文数大于配置的数目值之后立即生效；
- 更新方式由基于报文数更新改为基于时间更新，则基于时间方式立即生效。

【举例】

配置基于时间的 GTK 更新方法。

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

```
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey method time-based 3600
```

配置基于数据包的 GTK 更新方法。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey method packet-based 600000
```

【相关命令】

- **gtk-rekey enable**

1.1.6 key-derivation

key-derivation 命令用来配置密钥衍生算法。

undo key-derivation 命令用来恢复缺省情况。

【命令】

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

【缺省情况】

密钥衍生算法为 **sha1**。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

sha1：表示 SHA1 算法，它使用 HMAC-SHA1 算法进行迭代计算产生密钥。

sha1-and-sha256：表示 SHA1 和 SHA256 算法，它使用 HMAC-SHA1 或 HMAC-SHA256 算法进行迭代计算产生密钥。

sha256：表示 SHA256 算法，它使用 HMAC-SHA256 算法进行迭代计算产生密钥。

【使用指导】

当使用 RSNA 安全机制，密钥衍生算法才会生效。

如果配置保护管理帧功能为 **mandatory** 模式，建议指定密钥衍生类型为 **sha256**。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

配置密钥衍生算法为 SHA256。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] key-derivation sha256
```

【相关命令】

- **akm mode**
- **cipher-suite**

- **security-ie**

1.1.7 pmf

pmf 命令用来开启保护管理帧功能。

undo pmf 命令用来关闭保护管理帧功能。

【命令】

pmf { **mandatory** | **optional** }

undo pmf

【缺省情况】

保护管理帧功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

mandatory：指定保护管理帧功能为强制模式，即不支持保护管理帧功能的客户端无法接入。

optional：指定保护管理帧功能为可选模式，即支持或不支持保护管理帧功能的客户端均可接入。

【使用指导】

当使用 RSNA 安全机制且配置了 CCMP 加密套件和 RSN 安全信息元素时，保护管理帧功能才会生效。

【举例】

开启保护管理帧功能。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf optional
```

【相关命令】

- **security-ie**
- **cipher-suite**

1.1.8 pmf association-comeback

pmf association-comeback 命令用来配置保护管理帧的关联返回时间。

undo pmf association-comeback 命令用来恢复缺省情况。

【命令】

pmf association-comeback *time*

undo pmf association-comeback

【缺省情况】

保护管理帧的关联返回时间为 1 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：保护管理帧的关联返回时间，取值范围为 1～20，单位为秒。

【使用指导】

如果 AP 拒绝客户端的关联/重关联请求帧，会向客户端发送关联/重关联响应帧，其中携带了保护管理帧关联返回时间。到了保护管理帧关联返回时间，AP 才会接收客户端的关联/重关联请求帧。

【举例】

配置保护管理帧的关联返回时间为 2 秒。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf association-comeback 2
```

1.1.9 pmf saquery retrycount

pmf saquery retrycount 命令用来配置 AP 发送 SA Query request 的最大重传次数。

undo pmf saquery retrycount 命令用来恢复缺省情况。

【命令】

pmf saquery retrycount *count*

undo pmf saquery retrycount

【缺省情况】

AP 发送 SA Query request 帧的最大重传次数为 4 次。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

count：表示 AP 发送 SA Query request 帧的最大重传次数，取值范围为 1～16。

【使用指导】

若 AP 在 SA Query 重试次数内未收到 SA Query 响应帧，并且关联返回时间已经超时，则 AP 将认为客户端已经掉线。

【举例】

设置 AP 发送 SA Query request 帧的最大重传次数为 3。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf saquery retrycount 3
```

【相关命令】

- **pmf**
- **pmf saquery retrycount**

1.1.10 pmf saquery retrytimeout

pmf saquery retrytimeout 命令用来设置 AP 发送 SA Query request 帧的时间间隔。

undo pmf saquery retrytimeout 命令用来恢复缺省情况。

【命令】

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

【缺省情况】

AP 发送 SA Query request 帧的时间间隔为 200 毫秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

timeout：指定 AP 发送 SA Query request 帧的时间间隔，取值范围为 100～500，单位为毫秒。

【举例】

设置 AP 发送 SA Query request 帧的时间间隔为 300 毫秒。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf saquery retrytimeout 300
```

【相关命令】

- **pmf**
- **pmf saquery retrytimeout**

1.1.11 preshared-key

preshared-key 命令用来配置 PSK 密钥。

undo preshared-key 命令用来恢复缺省情况。

【命令】

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

【缺省情况】

未配置 PSK 密钥。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

pass-phrase：以字符串方式输入预共享密钥。

raw-key：以十六进制数方式输入预共享密钥。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。密钥长度的范围与选择的密钥参数有关，具体关系如下：

- 对于 **pass-phrase**，明文密钥为 8～63 个字符的字符串，密文密钥为 8～117 个字符的字符串。
- 对于 **raw-key**，明文密钥为 64 个十六进制数，密文密钥为 8～117 个字符的字符串。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。只有认证密钥管理模式为 PSK 时，此命令才能够生效，当认证密钥管理模式为 802.1X 时，配置了此项，无线服务模板可以使能，但此配置不会生效。

PSK 密钥只能配置一个。

【举例】

配置使用明文字符串 12345678 作为 PSK 密钥。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] akm mode psk
[Sysname-wlan-st-security] preshared-key pass-phrase simple 12345678
```

【相关命令】

- **akm mode**

1.1.12 ptk-lifetime

ptk-lifetime 命令用来配置 PTK 的生存时间。

undo ptk-lifetime 命令用来恢复缺省情况。

【命令】

ptk-lifetime *time*

undo ptk-lifetime

【缺省情况】

PTK 的生存时间为 43200 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：指定生存时间，取值范围为 180～604800，单位为秒。

【使用指导】

若该命令在无线服务模板处于开启状态下配置，则在原有定时器超时后，该配置生效。

【举例】

配置 PTK 生存时间为 200 秒。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] ptk-lifetime 200
```

1.1.13 ptk-rekey enable

ptk-rekey enable 命令用来开启 PTK 更新功能。

undo ptk-rekey enable 命令用来关闭 PTK 更新功能。

【命令】

ptk-rekey enable

undo ptk-rekey enable

【缺省情况】

PTK 更新功能处于开启状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

PTK 更新是对单播数据报文的加密密钥进行更新的一种安全手段，采用重新进行四次握手协商出新的 PTK 密钥的更新机制。

开启本功能后，设备会按照 **ptk-lifetime** 命令配置的生存时间周期性的更新 PTK。

【举例】

开启 PTK 更新功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] ptk-rekey enable
```

【相关命令】

- **ptk-lifetime**

1.1.14 security-ie

security-ie 命令用来配置信标和探查响应帧携带安全 IE。

undo security-ie 命令用来配置信标和探查响应帧不携带指定的安全 IE。

【命令】

security-ie { **rsn** | **wpa** } *

undo security-ie { **rsn** | **wpa** } *

【缺省情况】

信标和探查响应帧不携带 WPA IE、RSN IE 或 OSEN IE。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

rsn：设置在 AP 发送信标和探查响应帧时携带 RSN IE。RSN IE 通告了 AP 的 RSN 能力。

wpa：设置在 AP 发送信标和探查响应帧时携带 WPA IE。WPA IE 通告了 AP 的 WPA 能力。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置，并且必须要配置 CCMP 或 TKIP 加密套件。

当 WLAN 网络采用 RSNA 安全机制时，必须配置安全 IE。

【举例】

配置信标帧和探查响应帧携带 RSN 信息元素。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] security-ie rsn
```

【相关命令】

- **akm mode**
- **cipher-suite**

1.1.15 snmp-agent trap enable wlan usersec

snmp-agent trap enable wlan usersec 命令用来开启用户安全的告警功能。

undo snmp-agent trap enable wlan usersec 命令用来关闭用户安全的告警功能。

【命令】

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

【缺省情况】

用户安全的告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启了告警功能之后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。（有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。）

【举例】

开启用户安全的告警功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable wlan usersec
```

1.1.16 tkip-cm-time

tkip-cm-time 命令用来配置发起 TKIP 反制策略时间。

undo tkip-cm-time 命令用来恢复缺省情况。

【命令】

tkip-cm-time *time*

undo tkip-cm-time

【缺省情况】

发起 TKIP 反制策略时间为 0，即不启动反制策略。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：设置发起 TKIP 反制策略时间，取值范围为 0～3600，单位为秒。

【使用指导】

启动 TKIP 反制策略后，如果相邻两次 MIC 错误的时间间隔小于等于配置的时间，则会解除所有关联到该无线服务的客户端，并且只有在 TKIP 反制策略实施的时间（60 秒）后，才允许客户端重新建立关联。

只有在配置了 TKIP 加密套件时，此命令才能够生效。

若该命令在无线服务模板处于开启状态时配置，则原有定时器超时后，该配置生效。

【举例】

配置发起 TKIP 反制策略时间为 180 秒。

```
<Sysname> system-view
[Sysname] wlan service-template security
```

```
[Sysname-wlan-st-security] tkip-cm-time 180
```

【相关命令】

- **cipher-suite**

1.1.17 wep key

wep key 命令用来配置 WEP 密钥。

undo wep key 命令用来删除指定的 WEP 密钥。

【命令】

wep key *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo wep key *key-id*

【缺省情况】

未配置 WEP 密钥。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

key-id：密钥的 ID，取值范围为 1～4。

wep40：设置 WEP40 密钥选项。

wep104：设置 WEP104 密钥选项。

wep128：设置 WEP128 密钥选项。

pass-phrase：表示共享密钥为字符串。

raw-key：表示共享密钥为十六进制数。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥的长度范围和选择的密钥参数有关，具体关系如下。密文密钥为 37～73 个字符的字符串。

- 对于 **wep40 pass-phrase**，明文密钥为 5 个字符的字符串。
- 对于 **wep104 pass-phrase**，明文密钥为 13 个字符的字符串。
- 对于 **wep128 pass-phrase**，明文密钥为 16 个字符的字符串。
- 对于 **wep40 raw-key**，明文密钥为 10 个 16 进制数。
- 对于 **wep104 raw-key**，明文密钥为 26 个 16 进制数。
- 对于 **wep128 raw-key**，明文密钥为 32 个 16 进制数。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

WEP 密钥只有在配置了 WEP 加密套件的前提下才生效，最多可以配置四个 WEP 密钥。

【举例】

配置加密套件为 WEP40，并配置 WEP40 密钥为明文 12345。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345
```

【相关命令】

- **cipher-suite**
- **wep key-id**

1.1.18 wep key-id

wep key-id 命令用来选用 WEP 密钥。

undo wep key-id 命令用来恢复缺省情况。

【命令】

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

【缺省情况】

WEP 加密使用的密钥 ID 为 1。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

1：选择密钥 ID 为 1。

2：选择密钥 ID 为 2。

3：选择密钥 ID 为 3。

4：选择密钥 ID 为 4。

【使用指导】

如果使用 RSNA 安全机制，密钥 ID 不能为 1，需要配置其它密钥索引值。因为 RSN 和 WPA 协商的密钥 ID 将为 1。本命令只能在无线服务模板处于关闭状态时配置。

只有在配置了与密钥长度相对应的 WEP 加密套件时，指定 ID 的密钥才会生效。

当配置了多个密钥，可以通过配置密钥 ID 选择要使用的加密密钥。

【举例】

配置 WEP40 加密套件，WEP40 密钥为明文 12345，配置密钥 ID 为 1。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] cipher-suite wep40
[Sysname-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345
[Sysname-wlan-st-security] wep key-id 1
```

【相关命令】

- **wep key**

1.1.19 wep mode dynamic

wep mode dynamic 命令用来开启动态 WEP 加密机制。

undo wep mode dynamic 命令用来关闭动态 WEP 加密机制。

【命令】

wep mode dynamic

undo wep mode dynamic

【缺省情况】

动态 WEP 加密机制处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

配置动态 WEP 加密必须和 dot1x 用户接入认证模式一起使用，并且 **wep key-id** 不能配置为 4。

【举例】

开启动态 WEP 加密机制。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] wep mode dynamic
```

【相关命令】

- **cipher-suite**
- **client-security authentication-mode**（用户接入与认证命令参考-WLAN 用户接入认证）
- **wep key**
- **wep key-id**

1.1.20 wlan password-failure-limit enable

wlan password-failure-limit enable 命令用来开启密码错误限制功能。

undo wlan password-failure-limit enable 命令用来关闭密码错误限制功能。

【命令】

wlan password-failure-limit enable [**detection-period** *detection-period*] [**failure-threshold** *failure-threshold*]

undo wlan password-failure-limit enable

【缺省情况】

密码错误限制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

detection-period *detection-period*：指定密码错误限制功能的检测周期，取值范围是 5～600，单位为秒，缺省值为 100。

failure-threshold *failure-threshold*：指定密码错误限制功能的检测阈值，取值范围是 1～100，缺省值为 20。

【使用指导】

开启本功能后，在指定检测周期内密码校验失败次数达到指定上限时，客户端会被立即加入到动态黑名单中。有关动态黑名单的详细介绍请参见“WLAN 配置指导”中的“WLAN 接入”。

只有当身份认证与密钥管理模式为 PSK 或者 Private-PSK 时，密码错误限制功能才会生效。

本功能仅对在设备上进行关联的新接入的无线客户端生效。

当 STAMGR 进程重启（例如：设备重启导致的 STAMGR 进程重启）后，本功能将对密码校验失败次数重新进行计数。

本功能不支持 IRF 组网中 AP 直接从备份 AC 上线的情况。

【举例】

配置无线客户端的密码错误限制检测周期为 300 秒，检测阈值为 50 次。

```
<Sysname> system-view
[Sysname] wlan password-failure-limit enable detection-period 300 failure-threshold 50
```

目 录

1 WIPS

1.1 WIPS配置命令

1.1.1 access-scan

access-scan enable 命令用来开启 Sensor 在接入时间段内执行 WIPS 扫描功能。

undo access-scan enable 命令用来关闭 Sensor 在接入时间段内执行 WIPS 扫描功能。

【命令】

access-scan enable

undo access-scan enable

【缺省情况】

Sensor 在接入时间段内执行 WIPS 扫描功能处于关闭状态。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【使用指导】

Sensor 在接入时间段内开启 WIPS 扫描后，WIPS 的检测和防御效果将会增强，但同时无线客户端的接入能力将减弱。

【举例】

开启 Sensor 在接入时间段内的 WIPS 扫描功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] access-scan enable
```

1.1.2 ap-channel-change

ap-channel-change 命令用来开启 AP 信道变化检测功能。

undo ap-channel-change 命令用来关闭 AP 信道变化检测功能。

【命令】

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

【缺省情况】

AP 信道变化检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到 AP 信道变化，设备也不会发送告警日志。

【举例】

开启 AP 信道变化的检测功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-channel-change quiet 5
```

1.1.3 ap-classification rule

ap-classification rule 命令用来创建 AP 分类规则，并进入 AP 分类规则视图。如果指定 ID 的 AP 分类规则已经存在，则直接进入 AP 分类规则视图。

undo ap-classification rule 命令用来删除指定的 AP 分类规则。

【命令】

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

【缺省情况】

不存在 AP 分类规则。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

rule-id：AP 分类规则的 ID，取值范围为 1～65535。

【举例】

创建并进入 ID 为 1 的 AP 分类规则视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
```

1.1.4 ap-flood

ap-flood 命令用来开启 AP 泛洪攻击检测功能。

undo ap-flood 命令用来关闭 AP 泛洪攻击检测功能。

【命令】

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

【缺省情况】

AP 泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

apnum *apnum-value*：无线网络中 AP 设备的基准值，取值范围为 10～200，缺省值为 80。

exceed *exceed-value*：允许超过基准值的最大个数，取值范围为 10～200，缺省值为 80。当检测到 AP 设备数量超过基准值与允许超过基准值的最大个数之和，即判定设备受到 AP 泛洪攻击，设备会发送告警日志。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到 AP 泛洪攻击，设备也不会发送告警日志。

【举例】

开启 AP 泛洪攻击检测功能，AP 设备的基准值为 50，允许超过基准值的最大个数为 50，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100
```

1.1.5 ap-impersonation

ap-impersonation 命令用来开启 AP 扮演者攻击检测功能。

undo ap-impersonation 命令用来关闭 AP 扮演者攻击检测功能。

【命令】

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

【缺省情况】

AP 扮演者攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的 AP 扮演者攻击达到告警阈值，也不会发送告警日志。

【举例】

在名称为 home 的分类策略中开启 AP 扮演者攻击检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-impersonation quiet 360
```

1.1.6 ap-rate-limit

ap-rate-limit 命令用来配置 AP 表项学习的速率。

undo ap-rate-limit 命令用来恢复缺省情况。

【命令】

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

【缺省情况】

学习 AP 表项的统计周期为 60 秒，发送告警信息后的静默时间为 1200 秒，AP 表项的阈值为 64。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：学习 AP 表项的统计周期，取值范围为 1～3600，单位为秒。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 1200～3600，单位为秒。在静默期间，设备停止学习新的 AP 表项，也不会发送告警信息。

threshold *threshold-value*：AP 表项的阈值，取值范围为 1～4096。当设备在一个统计周期内学习 AP 表项达到触发阈值，设备会发送告警信息。

【举例】

配置 AP 表项学习的速率，学习 AP 表项的统计周期为 60 秒，发送告警信息后的静默时间为 1600 秒，AP 表项的阈值为 100。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100
```

【相关命令】

- **ap-timer**

1.1.7 ap-spoofing

ap-spoofing 命令用来开启 AP 地址仿冒检测功能。

undo ap-spoofing 命令用来关闭 AP 地址仿冒检测功能。

【命令】

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

【缺省情况】

AP 地址仿冒检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600 秒。在静默期间，设备再次检测到 AP 地址仿冒也不会发送告警信息。

【使用指导】

开启本功能后，如果设备检测到 AP 地址仿冒，则会发送告警信息。

【举例】

开启 AP 地址仿冒检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-spoofing quiet 360
```

1.1.8 ap-timer

ap-timer 命令用来配置 AP 表项的时间参数。

undo ap-timer 命令用来恢复缺省情况。

【命令】

ap-timer inactive *inactive-value* **aging** *aging-value*

undo ap-timer

【缺省情况】

AP 表项的非活跃时间为 300 秒，老化时间为 600 秒。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

inactive *inactive-value*：非活跃时间，取值范围为 60～1200，单位为秒。

aging *aging-value*：老化时间，取值范围为 120～86400，单位为秒。

【使用指导】

非活跃时间为从创建 AP 表项到其状态变为 Inactive 的时间；老化时间为从创建 AP 表项到删除 AP 表项的时间。

配置的老化时间必须大于非活跃时间。

【举例】

配置 AP 表项的时间参数，非活跃时间为 120 秒，老化时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ap-timer inactive 120 aging 360
```

【相关命令】

- **ap-rate-limit**

1.1.9 apply ap-classification rule

apply ap-classification rule 命令用来在分类策略中应用 AP 分类规则。

undo apply ap-classification rule 命令用来取消应用的 AP 分类规则。

【命令】

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

【缺省情况】

分类策略中没有应用 AP 分类规则。

【视图】

分类视图

【缺省用户角色】

network-admin

【参数】

rule-id：AP 分类规则的 ID，取值范围为 1～65535。

authorized-ap：通过合法认证的 AP。

external-ap：外部的 AP。

misconfigured-ap：错误配置的 AP。

rogue-ap：非法的 AP。

level：应用 AP 分类规则后设置的 AP 危险级别，取值范围为 1～100，缺省值为 50。

【举例】

将 ID 为 1 的 AP 分类规则应用到名称为 home 的分类策略内，并将 AP 分类为非法的 AP，危险级别定义为 80。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80
```

【相关命令】

- **ap-classification rule**

1.1.10 apply classification policy

apply classification policy 命令用来在 VSD（Virtual Security Domain，虚拟安全域）上应用分类策略。

undo apply classification policy 命令用来取消应用的分类策略。

【命令】

apply classification policy *policy-name*

undo apply classification policy *policy-name*

【缺省情况】

没有在 VSD 上应用分类策略。

【视图】

VSD 视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

在 VSD 上应用分类策略 policy1。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] virtual-security-domain home
[Sysname-wips-vsd-home] apply classification policy policy1
```

1.1.11 apply countermeasure policy

apply countermeasure policy 命令用来在 VSD 上应用反制策略。

undo apply countermeasure policy 命令用来取消应用的反制策略。

【命令】

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

【缺省情况】

没有在 VSD 上应用反制策略。

【视图】

VSD 视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

在 VSD 上应用反制策略 policy2。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] virtual-security-domain home
[Sysname-wips-vsd-home] apply countermeasure policy policy2
```

1.1.12 apply detect policy

apply detect policy 命令用来在 VSD 上应用攻击检测策略。

undo apply detect policy 命令用来取消应用的攻击检测策略。

【命令】

apply detect policy *policy-name*

undo apply detect policy *policy-name*

【缺省情况】

没有在 VSD 上应用攻击检测策略。

【视图】

VSD 视图

【缺省用户角色】

network-admin

【参数】

policy-name：攻击检测策略名称，为 1～63 个字符的字符串，区分大小写。

【举例】

在 VSD 上应用攻击检测策略 policy2。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] virtual-security-domain home
[Sysname-wips-vsd-home] apply detect policy policy2
```

1.1.13 apply signature policy

apply signature policy 命令用来在 VSD 内应用 Signature 策略。

undo apply signature policy 命令用来取消应用的 Signature 策略。

【命令】

apply signature policy *policy-name*

undo apply signature policy *policy-name*

【缺省情况】

VSD 内没有应用 Signature 策略。

【视图】

VSD 视图

【缺省用户角色】

network-admin

【参数】

policy-name：Signature 策略的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

将名为 policy1 的 Signature 策略应用到名为 home 的 VSD 内。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] virtual-security-domain home
[Sysname-wips-vsd-home] apply signature policy policy1
```

1.1.14 apply signature rule

apply signature rule 命令用来在 Signature 策略中应用 Signature 规则。

undo apply signature rule 命令用来取消应用的 Signature 规则。

【命令】

apply signature rule *rule-id*

undo apply signature rule *rule-id*

【缺省情况】

Signature 策略中没有应用 Signature 规则。

【视图】

Signature 策略视图

【缺省用户角色】

network-admin

【参数】

rule-id：规则的规则编号值，取值范围为 1～65535。

【举例】

配置 Signature 策略 office 中应用 ID 为 1 的 Signature 规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature policy office
[Sysname-wips-sig-office] apply signature rule 1
```

1.1.15 association-table-overflow

association-table-overflow 命令用来开启关联/重关联 DoS 攻击检测功能。

undo association-table-overflow 命令用来关闭关联/重关联 DoS 攻击检测功能。

【命令】

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

【缺省情况】

关联/重关联 DoS 攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到关联/重关联 DoS 攻击，设备也不会发送告警日志。

【举例】

配置开启关联/重关联 DoS 攻击检测功能，静默时间为 100。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] association-table-overflow quiet 100
```

1.1.16 authentication

authentication 命令用来在 AP 分类规则中对 AP 使用无线服务的安全认证方式进行匹配。

undo authentication 命令用来恢复缺省情况。

【命令】

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

【缺省情况】

没有在 AP 分类规则中对 AP 使用无线服务的安全认证方式进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

equal：匹配项与条件相同。

include：匹配项包含条件。

802.1x：认证方式为 802.1X 认证。

none：无认证。

other：认证方式为除 802.1X 和 PSK 之外的其他认证。

psk：认证方式为 PSK 认证。

【举例】

在 ID 为 1 的 AP 分类策略中对采用 PSK 认证方式接入无线网络的 AP 设备进行匹配。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] authentication equal psk
```

1.1.17 block mac-address

block mac-address 命令用来将指定的 MAC 地址添加到静态禁用设备列表中。

undo block mac-address 命令用来删除静态禁用设备列表中的 MAC 地址。

【命令】

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

【缺省情况】

静态禁用设备列表中不存在 MAC 地址。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【参数】

mac-address：AP 或客户端的 MAC 地址，格式为 H-H-H。

all：所有 MAC 地址。

【举例】

将 MAC 地址 78AC-C0AF-944F 添加到静态禁用设备列表中。

```
<Sysname> system-view
[Sysname] wips
```

```
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] block mac-address 78AC-C0AF-944F
```

1.1.18 classification policy

classification policy 命令用来创建分类策略，并进入分类策略视图。如果指定的分类策略已经存在，则直接进入分类策略视图。

undo classification policy 命令用来删除分类策略。

【命令】

classification policy *policy-name*

undo classification policy *policy-name*

【缺省情况】

不存在分类策略。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

创建名称为 home 的分类策略，并进入分类策略视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home]
```

1.1.19 client-association fast-learn enable

client-association fast-learn enable 命令用来开启 Sensor 快速学习客户端关联表项的功能。

undo client-association fast-learn enable 命令用来关闭 Sensor 快速学习客户端关联表项的功能。

【命令】

client-association fast-learn enable

undo client-association fast-learn enable

【缺省情况】

Sensor 快速学习客户端关联表项的功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【使用指导】

客户端关联表项是指客户端关联 AP 后在 AC 上建立的用于保存客户端信息的表项。

客户端关联 AP 时，需要向 AP 发送关联请求帧，然后 AP 向客户端发送关联响应帧，未开启本功能的情况下，Sensor 必须等 AP 向客户端发送关联响应帧，客户端与 AP 关联成功后，才能学习网络中客户端的关联表项。开启本功能后，Sensor 只需要在客户端发送关联请求帧或 AP 向客户端发送关联响应帧时，便可学习客户端关联表项，这样可以尽快学习到客户端关联表项，而不必等到一个完整的关联交互过程结束后。

如果 Sensor 在客户端发送关联请求帧时学习到了客户端关联表项，则在 AP 向客户端发送关联响应帧时会更新该表项，即每次检测到客户端发送给 AP 的关联请求帧或 AP 发送给客户端的关联响应帧时，都会更新客户端关联表项。

本功能虽然可以提高 Sensor 学习客户端关联表项的效率，但同时会降低学习客户端关联表项的准确性，因此通常建议在需要快速检测网络中的攻击并进行反制的情况下开启本功能。

【举例】

开启 Sensor 快速学习客户端关联表项的功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy 1
[Sysname-wips-dtc-1] client-association fast-learn enable
```

1.1.20 client-online

client-online 命令用来在 AP 分类规则中对 AP 上已关联的无线客户端数量进行匹配。

undo client-online 命令用来恢复缺省情况。

【命令】

client-online *value1* [**to** *value2*]

undo client-online

【缺省情况】

没有在 AP 分类规则中对 AP 上已关联的无线客户端数量进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

value1：指定与 AP 关联的无线客户端数量。*value1* 的取值范围为 0～128。

to *value2*：与 *value1* 共同作用，指定与 AP 关联的无线客户端数量范围，*value2* 的取值范围为 0～128 且必须大于或等于 *value1*。

【举例】

在 ID 为 1 的 AP 分类规则中匹配关联的无线客户端的数量在 20～40 之间的 AP。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] client-online 20 to 40
```

1.1.21 client-rate-limit

client-rate-limit 命令用来配置客户端表项学习的速率。

undo client -rate-limit 命令用来恢复缺省情况。

【命令】

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

【缺省情况】

学习客户端表项的统计周期为 60 秒，发送告警信息后的静默时间为 1200 秒，客户端表项的阈值为 512。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：学习客户端表项的统计周期，取值范围为 1～3600，单位为秒。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 1200～3600，单位为秒。在静默期间，设备停止学习新的客户端表项，也不会发送告警信息。

threshold *threshold-value*：客户端表项的阈值，取值范围为 1～4096。当设备在一个统计周期内学习客户端表项达到触发阈值，设备会发送告警信息。

【举例】

配置客户端表项学习的速率，学习客户端表项的统计周期为 80 秒，发送告警信息后的静默时间为 1600 秒，客户端表项的阈值为 100。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] client-rate-limit interval 80 threshold 100 quiet 1600
```

【相关命令】

- **client-timer**

1.1.22 client-spoofing

client-spoofing 命令用来开启客户端地址仿冒检测功能。

undo client-spoofing 命令用来关闭客户端地址仿冒检测功能。

【命令】

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

【缺省情况】

客户端地址仿冒检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600 秒。在静默期间，设备再次检测到客户端地址仿冒也不会发送告警信息。

【使用指导】

设备检测到客户端地址仿冒后会发送告警信息。

【举例】

开启客户端地址仿冒检测功能，配置发送告警信息后的静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] client-spoofing quiet 360
```

1.1.23 client-timer

client-timer 命令用来配置客户端表项的时间参数。

undo client-timer 命令用来恢复缺省情况。

【命令】

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

【缺省情况】

客户端表项的非活跃时间为 300 秒，老化时间为 600 秒。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

inactive *inactive-value*：从创建客户端表项到非活跃状态的时间，即非活跃时间，取值范围为 60～1200，单位为秒。

aging *aging-value*：从创建客户端表项到删除客户端表项的时间，即老化时间，取值范围为 120～86400，单位为秒。

【使用指导】

配置的老化时间必须大于非活跃时间。

【举例】

配置客户端表项的时间参数，非活跃时间为 120 秒，老化时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] client-timer inactive 120 aging 360
```

【相关命令】

- **client-rate-limit**

1.1.24 countermeasure adhoc

countermeasure adhoc 命令用来配置对 ad hoc 设备进行反制。

undo countermeasure adhoc 命令用来恢复缺省情况。

【命令】

countermeasure adhoc

undo countermeasure adhoc

【缺省情况】

未配置对 ad hoc 设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对 ad hoc 设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure adhoc
```

1.1.25 countermeasure attack all

countermeasure attack all 命令用来配置对所有发起攻击的设备进行反制。

undo countermeasure attack all 命令用来恢复缺省情况。

【命令】

countermeasure attack all

undo countermeasure attack all

【缺省情况】

未配置对所有发起攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对所有发起攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack all
```

1.1.26 countermeasure attack deauth-broadcast

countermeasure attack deauth-broadcast 命令用来配置对发起广播解除认证帧攻击的设备进行反制。

undo countermeasure deauth-broadcast 命令用来恢复缺省情况。

【命令】

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

【缺省情况】

未配置对发起广播解除认证帧攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起广播解除认证帧攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack deauth-broadcast
```

1.1.27 countermeasure attack disassoc-broadcast

countermeasure attack disassoc-broadcast 命令用来配置对发起广播解除关联帧攻击的设备进行反制。

undo countermeasure attack disassoc-broadcast 命令用来恢复缺省情况。

【命令】

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

【缺省情况】

未配置对发起广播解除关联帧攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起广播解除关联帧攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack disassoc-broadcast
```

1.1.28 countermeasure attack honeypot-ap

countermeasure attack honeypot-ap 命令用来配置对发起蜜罐 AP 攻击的设备进行反制。

undo countermeasure attack honeypot-ap 命令用来恢复缺省情况。

【命令】

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

【缺省情况】

未配置对发起蜜罐 AP 攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起蜜罐 AP 攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
```

```
[Sysname-wips-cms-home] countermeasure attack honeypot-ap
```

1.1.29 countermeasure attack hotspot-attack

countermeasure attack hotspot-attack 命令用来配置对发起热点攻击的设备进行反制。

undo countermeasure attack hotspot-attack 命令用来恢复缺省情况。

【命令】

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

【缺省情况】

未配置对发起热点攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起热点攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack hotspot-attack
```

1.1.30 countermeasure attack ht-40-mhz-intolerance

countermeasure attack ht-40-mhz-intolerance 命令用来配置对禁用 802.11n 40MHz 模式的设备进行反制。

undo countermeasure attack ht-40-mhz-intolerance 命令用来恢复缺省情况。

【命令】

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

【缺省情况】

未配置对禁用 802.11n 40MHz 模式的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对禁用 802.11n 40MHz 模式的设备进行反制。

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

```
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack ht-40-mhz-intolerance
```

1.1.31 countermeasure attack malformed-packet

countermeasure attack malformed-packet 命令用来配置对发起畸形报文攻击的设备进行反制。

undo countermeasure attack malformed-packet 命令用来恢复缺省情况。

【命令】

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

【缺省情况】

未配置对发起畸形报文攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起畸形报文攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack malformed-packet
```

1.1.32 countermeasure attack man-in-the-middle

countermeasure attack man-in-the-middle 命令用来配置对发起中间人攻击的设备进行反制。

undo countermeasure attack man-in-the-middle 命令用来恢复缺省情况。

【命令】

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

【缺省情况】

未配置对发起中间人攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起中间人攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack man-in-the-middle
```

1.1.33 countermeasure attack omerta

countermeasure attack omerta 命令用来配置对发起 Omerta 攻击的设备进行反制。

undo countermeasure attack omerta 命令用来恢复缺省情况。

【命令】

countermeasure attack omerta

undo countermeasure attack omerta

【缺省情况】

未配置对发起 Omerta 攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起 Omerta 攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack omerta
```

1.1.34 countermeasure attack power-save

countermeasure attack power-save 命令用来配置对发起节电攻击的设备进行反制。

undo countermeasure attack power-save 命令用来恢复缺省情况。

【命令】

countermeasure attack power-save

undo countermeasure attack power-save

【缺省情况】

未配置对发起节电攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起节电攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack power-save
```

1.1.35 countermeasure attack soft-ap

countermeasure attack soft-ap 命令用来配置对发起软 AP 攻击的设备进行反制。

undo countermeasure attack soft-ap 命令用来恢复缺省情况。

【命令】

countermeasure attack soft-ap

undo countermeasure attack soft-ap

【缺省情况】

未配置对发起软 AP 攻击的设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对发起软 AP 攻击的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack soft-ap
```

1.1.36 countermeasure attack unencrypted-trust-client

countermeasure attack unencrypted-trust-client 命令用来配置对未加密的信任客户端进行反制。

undo countermeasure attack unencrypted-trust-client 命令用来恢复缺省情况。

【命令】

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

【缺省情况】

未配置对未加密的信任客户端进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对未加密的信任客户端进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack unencrypted-trust-client
```

1.1.37 countermeasure attack weak-iv

countermeasure attack weak-iv 命令用来配置对 Weak IV 设备进行反制。

undo countermeasure weak-iv 命令用来恢复缺省情况。

【命令】

countermeasure attack weak-iv

undo countermeasure attack weak-iv

【缺省情况】

未配置对 Weak IV 设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对 Weak IV 设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack weak-iv
```

1.1.38 countermeasure attack windows-bridge

countermeasure attack windows-bridge 命令用来配置对 Windows 网桥设备进行反制。

undo countermeasure attack windows-bridge 命令用来恢复缺省情况。

【命令】

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

【缺省情况】

未配置对 Windows 网桥设备进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

配置对 Windows 网桥设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure attack windows-bridge
```

1.1.39 countermeasure external-ap

countermeasure external-ap 命令用来配置对外部 AP 进行反制。

undo countermeasure external-ap 命令用来恢复缺省情况。

【命令】

countermeasure external-ap

undo countermeasure external-ap

【缺省情况】

未配置对外部 AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对外部 AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure external-ap
```

1.1.40 countermeasure mac-address

countermeasure mac-address 命令用来配置根据指定的 MAC 地址对设备进行手工反制。

undo countermeasure mac-address 命令用来取消根据指定的 MAC 地址对设备进行手工反制。

【命令】

countermeasure mac-address *mac-address*

undo countermeasure mac-address { *mac-address* | **all** }

【缺省情况】

未配置根据指定的 MAC 地址对设备进行手工反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【参数】

mac-address：AP 或客户端的 MAC 地址，格式为 H-H-H。

all：表示所有 AP 或客户端的 MAC 地址。

【使用指导】

可以通过配置多条该命令对多个设备进行手工反制。

【举例】

配置对 MAC 地址为 2a11-1fa1-141f 的设备进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f
```

1.1.41 countermeasure misassociation-client

countermeasure misassociation-client 命令用来配置对关联错误的客户端进行反制。

undo countermeasure misassociation-client 命令用来恢复缺省情况。

【命令】

countermeasure misassociation-client

undo countermeasure misassociation-client

【缺省情况】

未配置对关联错误的客户端进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对关联错误的客户端进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure misassociation-client
```

1.1.42 countermeasure misconfigured-ap

countermeasure misconfigured-ap 命令用来配置对配置错误的 AP 进行反制。

undo countermeasure misconfigured-ap 命令用来恢复缺省情况。

【命令】

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

【缺省情况】

未配置对配置错误的 AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对配置错误的 AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure misconfigured-ap
```

1.1.43 countermeasure policy

countermeasure policy 命令用来创建反制策略，并进入反制策略视图。如果指定的反制策略已经存在，则直接进入反制策略视图。

undo countermeasure policy 命令用来删除反制策略。

【命令】

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

【缺省情况】

不存在反制策略。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

policy-name：反制策略的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

创建名称为 home 的反制策略，并进入反制策略视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home]
```

1.1.44 countermeasure potential-authorized-ap

countermeasure potential-authorized-ap 命令用来配置对潜在授权 AP 进行反制。

undo countermeasure potential-authorized-ap 命令用来恢复缺省情况。

【命令】

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

【缺省情况】

未配置对潜在授权 AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对潜在授权 AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure potential-authorized-ap
```

1.1.45 countermeasure potential-external-ap

countermeasure potential-external-ap 命令用来配置对潜在外部 AP 进行反制。

undo countermeasure potential-external-ap 命令用来恢复缺省情况。

【命令】

countermeasure potential-external-ap

undo countermeasure potential-external-ap

【缺省情况】

未配置对潜在外部 AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对潜在外部 AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure potential-external-ap
```

1.1.46 countermeasure potential-rogue-ap

countermeasure potential-rogue-ap 命令用来配置对潜在 Rogue AP 进行反制。

undo countermeasure potential-rogue-ap 命令用来恢复缺省情况。

【命令】

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

【缺省情况】

未配置对潜在 Rogue AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对潜在 Rogue AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure potential-rogue-ap
```

1.1.47 countermeasure rogue-ap

countermeasure rogue-ap 命令用来配置对 Rogue AP 进行反制。

undo countermeasure rogue-ap 命令用来恢复缺省情况。

【命令】

countermeasure rogue-ap

undo countermeasure rogue-ap

【缺省情况】

未配置对 Rogue AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对 Rogue AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure rogue-ap
```

1.1.48 countermeasure unauthorized-client

countermeasure unauthorized-client 命令用来配置对未授权的客户端进行反制。

undo countermeasure unauthorized-client 命令用来恢复缺省情况。

【命令】

countermeasure unauthorized-client

undo countermeasure unauthorized-client

【缺省情况】

未配置对未授权的客户端进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对未授权的客户端进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure unauthorized-client
```

1.1.49 countermeasure uncategorized-ap

countermeasure uncategorized-ap 命令用来配置对未确定分类的 AP 进行反制。

undo countermeasure uncategorized-ap 命令用来恢复缺省情况。

【命令】

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

【缺省情况】

未配置对未确定分类的 AP 进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对未确定分类的 AP 进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure uncategorized-ap
```

1.1.50 countermeasure uncategorized-client

countermeasure uncategorized-client 命令用来配置对未确定分类的客户端进行反制。

undo countermeasure uncategorized-client 命令用来恢复缺省情况。

【命令】

countermeasure uncategorized-client

undo countermeasure uncategorized-client

【缺省情况】

未配置对未确定分类的客户端进行反制。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【举例】

对未确定分类的客户端进行反制。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-cms-home] countermeasure uncategorized-client
```

1.1.51 deauth-spoofing

deauth-spoofing 命令用来开启仿冒 Deauthentication 帧检测功能。

undo deauth-spoofing 命令用来关闭仿冒 Deauthentication 帧检测功能。

【命令】

deauth-spoofing [**quiet** *quiet*]

undo deauth-spoofing

【缺省情况】

仿冒 Deauthentication 帧检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到仿冒 Deauthentication 帧，设备也不会发送告警日志。

【举例】

开启仿冒 Deauthentication 帧检测功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] deauth-spoofing quiet 100
```

1.1.52 deauthentication-broadcast

deauthentication-broadcast 命令用来开启广播解除认证帧检测功能。

undo deauthentication-broadcast 命令用来关闭广播解除认证帧检测功能。

【命令】

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

【缺省情况】

广播解除认证帧检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测广播解除认证帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的广播解除认证帧的数量达到触发告警阈值，设备也不会发送告警日志。

threshold *threshold-value*：检测广播解除认证帧达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的广播解除认证帧的数量达到触发告警阈值，即判定设备检测到广播解除认证帧，设备会发送告警日志。

【举例】

配置检测广播解除认证帧功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360
```

1.1.53 detect dissociate-client enable

detect dissociate-client enable 命令用来开启 WIPS 检测游离客户端功能。

undo detect dissociate-client enable 命令用来关闭 WIPS 检测游离客户端功能。

【命令】

detect dissociate-client enable

undo detect dissociate-client enable

【缺省情况】

WIPS 检测游离客户端功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【举例】

开启 WIPS 检测游离客户端功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] detect dissociate-client enable
```

1.1.54 detect policy

detect policy 命令用来创建攻击检测策略，并进入攻击检测策略视图，如果指定的攻击检测策略已经存在，则直接进入攻击检测策略视图。

undo detect policy 命令用来删除攻击检测策略。

【命令】

detect policy *policy-name*

undo detect policy *policy-name*

【缺省情况】

不存在攻击检测策略。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

policy-name：攻击检测策略的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

创建名称为 home 的攻击检测策略，并进入攻击检测策略视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home]
```

1.1.55 detect signature

detect signature 命令用来开启对符合 Signature 规则的报文检测功能。

undo detect signature 命令用来关闭对符合 Signature 规则的报文检测功能。

【命令】

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

【缺省情况】

对符合 Signature 规则的报文检测功能处于开启状态。

【视图】

Signature 策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：对符合 Signature 规则的报文检测的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省取值为 600。

threshold *threshold-value*：对符合 Signature 规则的报文检测达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备检测到符合 Signature 规则的报文的数量达到触发告警阈值，设备会发送告警日志。

【举例】

开启对符合 Signature 规则的报文检测功能，统计周期为 60 秒，统计次数的阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature policy home
[Sysname-wips-sig-home] detect signature interval 60 threshold 100 quiet 360
```

1.1.56 disassociation-broadcast

disassociation-broadcast 命令用来开启广播解除关联帧检测功能。

undo disassociation-broadcast 命令用来关闭广播解除关联帧检测功能。

【命令】

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

【缺省情况】

广播解除关联帧检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测广播解除关联帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的广播解除关联帧的数量达到触发告警阈值，设备也不会发送告警日志。

threshold *threshold-value*：检测广播解除关联帧达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的广播解除关联帧的数量达到触发告警阈值，即判定设备检测到广播解除关联帧，设备会发送告警日志。

【举例】

配置检测广播解除关联帧功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360
```

1.1.57 discovered-ap

discovered-ap 命令用来在 AP 分类规则中对发现 AP 的 Sensor 数量进行匹配。

undo discovered-ap 命令用来恢复缺省情况。

【命令】

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

【缺省情况】

没有在 AP 分类规则中对发现 AP 的 Sensor 数量进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

value1：指定匹配发现 AP 数量。*value1* 的取值范围为 1～128。

to *value2*：与 *value1* 共同作用，指定匹配发现 AP 数量范围，*value2* 的取值范围为 1～128 且必须大于或等于 *value1*。

【举例】

在 ID 为 1 的 AP 分类策略中配置对发现 AP 的 Sensor 数量大于 10 的 AP 进行匹配。

```
<Sysname> system-view
[Sysname] wips
```

```
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] discovered-ap 10 to 128
```

1.1.58 display wips sensor

display wips sensor 命令用来显示所有 Sensor 的信息。

【命令】

display wips sensor

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示所有 Sensor 的信息。

```
<Sysname> display wips sensor
Total number of sensors: 1
Sensor ID    Sensor name                VSD name                Radio ID   Status
1            fatap                      aaa                     1          Active
```

表1-1 display wips sensor 命令显示信息描述表

字段	描述
Sensor ID	Sensor设备的ID
Sensor name	Sensor设备的名称
VSD name	AP所在的虚拟安全域
Radio ID	开启WIPS的Radio ID
Status	Sensor的状态： • Active：已运行 WIPS 功能的 Sensor • Inactive：未运行 WIPS 功能的 Sensor

1.1.59 display wips statistics

display wips statistics 命令用来显示攻击检测统计信息。

【命令】

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

receive：所有虚拟安全域中的攻击检测统计信息。

virtual-security-domain *vsd-name*：指定虚拟安全域中的攻击检测统计。

【举例】

显示所有的虚拟安全域中的攻击检测统计信息。

```
<Sysname> display wips statistics receive
Information from sensor 1
 Information about attack statistics:
   Detected association-request flood messages: 0
   Detected authentication flood messages: 0
   Detected beacon flood messages: 0
   Detected block-ack flood messages: 0
   Detected cts flood messages: 0
   Detected deauthentication flood messages: 0
   Detected disassociation flood messages: 0
   Detected eapol-start flood messages: 0
   Detected null-data flood messages: 0
   Detected probe-request flood messages: 0
   Detected reassociation-request flood messages: 0
   Detected rts flood messages: 0
   Detected eapol-logoff flood messages: 0
   Detected eap-failure flood messages: 0
   Detected eap-success flood messages: 0
   Detected duplicated-ie messages: 0
   Detected fata-jack messages: 0
   Detected illegal-ibss-ess messages: 0
   Detected invalid-address-combination messages: 0
   Detected invalid-assoc-req messages: 0
   Detected invalid-auth messages: 0
   Detected invalid-deauth-code messages: 0
   Detected invalid-disassoc-code messages: 0
   Detected invalid-ht-ie messages: 0
   Detected invalid-ie-length messages: 0
   Detected invalid-pkt-length messages: 0
   Detected large-duration messages: 0
   Detected null-probe-resp messages: 0
   Detected overflow-eapol-key messages: 0
   Detected overflow-ssid messages: 0
   Detected redundant-ie messages: 0
   Detected AP spoof AP messages: 0
   Detected AP spoof client messages: 0
   Detected AP spoof ad-hoc messages: 0
   Detected ad-hoc spoof AP messages: 0
   Detected client spoof AP messages: 0
   Detected weak IV messages: 0
```

```
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassociation messages: 0
Detected broadcast deauthentication messages: 0
Detected AP impersonate messages: 0
Detected illegal channel 9 messages: 1
```

表1-2 display wips statistics 命令显示信息描述表

字段	描述
Information from sensor n	Sensor n发送的消息，n表示sensor ID
Information about attack statistics	关于攻击信息统计
Detected association-request flood messages	检测到关联请求帧的泛洪攻击消息的上报计数
Detected authentication flood messages	检测到鉴权帧的泛洪攻击消息的上报计数
Detected beacon flood messages	检测到Beacon帧的泛洪攻击消息的上报计数
Detected block-ack flood messages	检测到批量确认帧的泛洪攻击消息的上报计数
Detected cts flood messages	检测到允许发送帧的泛洪攻击消息的上报计数
Detected deauthentication flood messages	检测到解除鉴权帧的泛洪攻击消息的上报计数
Detected disassociation flood messages	检测到解除关联帧的泛洪攻击消息的上报计数
Detected eapol-start flood messages	检测到握手开始帧的泛洪攻击消息的上报计数
Detected null-data flood messages	检测到空数据帧的泛洪攻击消息的上报计数
Detected probe-request flood messages	检测到探查请求帧的泛洪攻击消息的上报计数
Detected reassociation-request flood messages	检测到重关联请求帧的泛洪攻击消息的上报计数
Detected rts flood messages	检测到请求发送帧的泛洪攻击消息的上报计数
Detected eapol-logoff flood messages	检测到下线请求帧的泛洪攻击消息的上报计数
Detected eap-failure flood messages	检测到失败类型认证帧的泛洪攻击消息的上报计数
Detected eap-success flood messages	检测到成功类型认证帧的泛洪攻击消息的上报计数
Detected duplicated-ie messages	检测到重复的IE畸形消息的上报计数
Detected fata-jack messages	检测到认证算法错畸形消息的上报计数
Detected illegal-ibss-ess messages	检测到无效IBSS-ESS畸形消息的上报计数

字段	描述
Detected invalid-address-combination messages	检测到无效联合地址畸形消息的上报计数
Detected invalid-assoc-req messages	检测到无效关联请求畸形消息的上报计数
Detected invalid-auth messages	检测到无效鉴权畸形消息的上报计数
Detected invalid-deauth-code messages	检测到无效解除鉴权码畸形消息的上报计数
Detected invalid-disassoc-code messages	检测到无效解除关联码畸形消息的上报计数
Detected invalid-ht-ie messages	检测到无效HT IE畸形消息的上报计数
Detected invalid-ie-length messages	检测到无效IE长度畸形消息的上报计数
Detected invalid-pkt-length messages	检测到无效报文长度畸形消息的上报计数
Detected large-duration messages	检测到超大持续时间畸形消息的上报计数
Detected null-probe-resp messages	检测到空探查响应畸形消息的上报计数
Detected overflow-eapol-key messages	检测到Eapol-key溢出畸形消息的上报计数
Detected overflow-ssid messages	检测到SSID溢出畸形消息的上报计数
Detected redundant-ie messages	检测到冗余的IE畸形消息的上报计数
Detected AP spoof AP messages	检测到AP仿冒AP消息的上报计数
Detected AP spoof client messages	检测到AP仿冒Client消息的上报计数
Detected AP spoof ad-hoc messages	检测到AP仿冒Ad-hoc消息的上报计数
Detected ad-hoc spoof AP messages	检测到Ad-hoc 仿冒AP消息的上报计数
Detected client spoof AP messages	检测到Client仿冒AP消息的上报计数
Detected weak IV messages	检测到弱向量消息的上报计数
Detected excess AP messages	检测到AP设备表项超过规格消息的上报计数
Detected excess client messages	检测到客户端设备表项超过规格消息的上报计数
Detected 40MHZ messages	检测到客户端禁用40MHz模式消息的上报计数
Detected power save messages	检测到节电攻击消息的上报计数
Detected omerta messages	检测到Omerta攻击消息的上报计数
Detected windows bridge messages	检测到Windows网桥消息的上报计数
Detected soft AP messages	检测到软AP消息的上报计数
Detected broadcast disassociation messages	检测到广播解除关联帧消息的上报计数
Detected broadcast deauthentication messages	检测到广播解除认证帧消息的上报计数
Detected AP impersonate messages	检测到AP扮演消息的上报计数
Detected illegal channel n messages:	检测到非法信道流量的计数，n表示信道号

【相关命令】

- **reset wips statistics**

1.1.60 display wips virtual-security-domain countermeasure record

display wips virtual-security-domain countermeasure record 命令用来显示指定VSD 内被反制过设备的信息。

【命令】

display wips virtual-security-domain *vsd-name* **countermeasure record**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

显示 VSD office 内被反制过设备的信息。

```
<Sysname> display wips virtual-security-domain office countermeasure record
Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain
office

Reason: Att - attack; Ass - associated; Black - blacklist;
        Class - classification; Manu - manual;

MAC address    Type   Reason   Countermeasure AP     Radio ID   Time
1000-0000-00e3 AP     Manu     fatap                  1          2016-05-03/09:32:01
1000-0000-00e4 AP     Manu     fatap                  1          2016-05-03/09:32:11
2000-0000-f282 Client Black    fatap                  1          2016-05-03/09:31:56
```

表1-3 display wips virtual-security-domain countermeasure record 命令显示信息描述表

字段	描述
Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office	累计成功通知反制次数；当前成功通知反制次数，最多可以显示1024条反制记录
MAC Address	检测到的无线设备的MAC地址
Type	无线设备的类型： • AP • Client

字段	描述
Reason	无线设备的反制原因： • Att：对发起攻击的设备进行的反制 • Class：根据设备分类类型进行的反制 • Manu：根据指定的 MAC 地址对设备进行手工反制
Countermeasure AP	发起反制设备的Sensor名称
Radio ID	发起反制设备的Sensor的Radio ID
Time	通知反制的时间

【相关命令】

- **reset wips virtual-security-domain countermeasure record**

1.1.61 display wips virtual-security-domain device

display wips virtual-security-domain device 命令用来显示指定 VSD 内检测到的无线设备的信息。

【命令】

display wips virtual-security-domain *vsd-name* **device** [**ap** [**ad-hoc** | **authorized** | **external** | **mesh** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue** | **uncategorized**] | **client** [[**dissociative-client**] | [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

device：显示所有设备的信息。

ap：显示检测到 AP 的信息。

ad-hoc：显示运行在 Ad hoc 模式的 AP 的信息。

authorized：显示授权 AP 的信息。

external：显示外部 AP 的信息。

mesh：显示 Mesh 链接的信息。

misconfigured：显示配置错误的 AP 的信息。

potential-authorized：显示潜在授权 AP 的信息。

potential-rogue：显示潜在 Rogue AP 的信息。

potential-external：显示潜在外部 AP 的信息。

rogue：显示 Rogue AP 的信息。

uncategorized：显示无法确定类别的 AP 的信息。

client：显示客户端的信息。

dissociative-client：显示游离客户端信息。

authorized：显示授权客户端的信息。

misassociation：显示误关联客户端的信息。

unauthorized：显示未授权客户端的信息。

uncategorized：显示无法确定类别的客户端的信息。

mac-address *mac-address*：显示指定 MAC 地址的无线设备的信息，*mac-address* 格式为 H-H-H。

verbose：显示检测到设备的详细信息。

【举例】

显示在虚拟安全域 office 内检测到的所有无线设备信息。

```
<Sysname> display wips virtual-security-domain office device
Total 3 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential;
       Ad-hoc; Mesh

MAC address    Type   Class    Duration    Sensors Channel Status
1000-0000-0000 AP     Ext(P)   00h 10m 46s 1       11      Active
1000-0000-0001 AP     Ext(P)   00h 10m 46s 1       6       Active
1000-0000-0002 AP     Ext(P)   00h 10m 46s 1       1       Active
```

表1-4 display wips virtual-security-domain device 命令显示信息描述表

字段	描述
MAC Address	检测到的无线设备的MAC地址
Type	无线设备的类型： • AP：AP 设备 • Client：无线客户端 • Mesh：无线网桥
Class	无线设备的分类类别，具体参见表1-5中的相关内容
Duration	无线设备的当前状态的持续时间
Sensors	检测到该无线设备的Sensor的数量
Channel	最后一次检测到该无线设备的信道

字段	描述
Status	AP或客户端表项的状态： • Active：AP 或客户端表项处于活跃状态 • Inactive：AP 或客户端表项处于非活跃状态

显示在虚拟安全域 a 内检测到的所有无线设备的详细信息。

```
<Sysname> display wips virtual-security-domain a device verbose
Total 2 detected devices in virtual-security-domain a

 AP: 1000-0000-0000
   Mesh Neighbor: None
   Classification: Mis(C)
   Severity level: 0
   Classify way: Auto
   Status: Active
   Status duration: 00h 27m 57s
   Vendor: Not found
   SSID: service
   Radio type: 802.11g
   Countermeasuring: No
   Security: None
   Encryption method: None
   Authentication method: None
   Broadcast SSID: Yes
   QoS supported: No
   Ad-hoc: No
   Beacon interval: 100 TU
   Up duration: 00h 27m 57s
Channel band-width supported: 20MHZ
   Hotspot AP: No
   Soft AP: No
   Honeypot AP: No
   Total number of reported sensors: 1
     Sensor 1:
       Sensor ID: 1
       Sensor name: fatap
       Radio ID: 1
       RSSI: 15
       Channel: 149
       First reported time: 2014-06-03/09:05:51
       Last reported time: 2014-06-03/09:05:51
   Total number of associated clients: 1
     01: 2000-0000-0000
Client: 2000-0000-0000
  Last reported associated AP: 1000-0000-0000
  Classification: Uncate
```

```
Severity level: 0
Classify way: Auto
Dissociative status: No
Status: Active
Status duration: 00h 00m 02s
Vendor: Not found
Radio type: 802.11a
40mhz intolerance: No
Countermeasuring: No
Man in the middle: No
Total number of reported sensors: 1
   Sensor 1:
     Sensor ID: 1
     Sensor name: fatap
     Radio ID: 1
     RSSI: 50
     Channel: 149
     First reported time: 2014-06-03/14:52:56
     Last reported time: 2014-06-03/14:52:56
     Reported associated AP: 1000-0000-0000
```

表1-5 display wips virtual-security-domain device verbose 命令显示信息描述表

字段	描述
Total *number* detected devices in virtual-security-domain *name*	在指定虚拟安全域内检测到无线设备的总数
AP	检测到AP的MAC地址
Mesh Neighbor	Mesh AP邻居的MAC地址
Client	检测到Client的MAC地址
Last reported associated AP	客户端最近一次上报关联AP的MAC地址

字段	描述

Classification	AP或无线客户端的分类：
	• 对于 AP 设备有以下几种：
	  ◦ ad_hoc：运行在 Ad hoc 模式的 AP
	  ◦ authorized：授权 AP
	  ◦ rogue：非法 AP
	  ◦ misconfigured：配置错误的 AP
	  ◦ external：外部 AP
	  ◦ potential-authorized：潜在授权的 AP
	  ◦ potential-rogue：潜在非法的 AP
	  ◦ potential-external：潜在外部的 AP
	  ◦ uncategorized：无法确认的 AP
	• 对于无线客户端有以下几种：
	  ◦ authorized：授权的客户端
	  ◦ unauthorized：未授权的客户端
	  ◦ misassociated：错误关联的客户端
	  ◦ uncategorized：未分类的客户端

Severity level	检测到设备的安全级别
Classify way	AP或无线客户端的分类方法： • Manual：手工分类 • Invalid OUI：导入无效 OUI 列表 • Block List：禁用列表 • Trust List：信任列表 • User Define：用户自定义分类 • Auto：自动分类
Dissociative status	是否是游离客户端
Status	AP或客户端表项的状态： • Active：AP 或客户端表项处于激活状态 • Inactive：AP 或客户端表项处于非激活状态
Status duration	设备当前状态的持续时间
Vendor	如果该设备的OUI能够匹配**`import oui`**命令导入配置文件中的OUI，则显示设备厂商，没有配置或者没有匹配到显示为Not found
SSID	AP提供的SSID
Radio Type	无线设备使用的射频模式
40MHz intolerance	客户端是否支持40MHz
Countermeasuring	设备是否被反制： • No：没有被反制或是已经被通知反制过 • Yes：正在被反制
Man in the middle	是否是中间人

字段	描述
Security	无线服务使用的安全方式： • None：未配置安全方式 • WEP：WEP（Wired Equivalent Privacy，有线等效加密）方式 • WPA：WPA（Wi-Fi Protected Access，WIFI 保护访问）方式 • WPA2：WPA 第二版方式
Encryption method	• 无线数据的加密方式： • TKIP：TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）加密 • CCMP：CCMP（Counter mode with CBC-MAC Protocol，[计数器模式]搭配[密码块链接－消息验证码]协议）加密 • WEP：WEP（Wired Equivalent Privacy，有线等效加密）加密 • None：无加密方式
Authentication method	AP提供的接入无线网络的认证方式： • None：无认证方式 • PSK：采用 PSK 认证方式 • 802.1X：采用 802.1X 认证方式 • Others：采用除 PSK 和 802.1X 之外的认证方式
Broadcast SSID	AP是否是广播SSID，如果AP不广播SSID，显示信息的SSID显示为空
QoS supported	是否支持QoS
Ad-hoc	是否是Ad hoc
Beacon interval	信标间隔，单位为TU，1TU等于1024微秒
Up duration	AP设备从启动到当前的持续时间
Channel band-width supported	支持的信道带宽： • 20/40/80MHZ：AP 支持 20MHz、40MHz 和 80MHz 的信道带宽 • 20/40MHZ：AP 支持 20MHz 和 40MHz 的信道带宽 • 20MHZ：AP 支持 20MHz 的信道带宽
Hotspot AP	是否是热点AP
Soft AP	是否是软AP
Honeypot AP	是否是蜜罐AP
Sensor *n*	发现该设备的Sensor，*n*为系统自动的编号
Sensor ID	Sensor的ID，即Sensor的APID
Sensor name	检测到该无线设备的Sensor的名称
Radio ID	发现该设备的Sensor上的Radio ID
RSSI	Sensor的信号强度
Channel	该Sensor最近一次探测到该设备的信道
First reported time	该Sensor第一次检测到该AP或无线客户端的时间

字段	描述
Last reported time	该Sensor最近一次检测到该AP或无线客户端的时间
Total number of associated clients	关联该设备的Client的数量
n: H-H-H	AP上关联的无线客户端的MAC地址，*n*为系统自动的编号
Reported associated AP	该Sensor上报关联AP的MAC地址

【相关命令】

- **reset wips virtual-security-domain device**

1.1.62 export oui

export oui 命令用来导出所有的 OUI 信息。

【命令】

export oui *file-name*

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

file-name：导出 OUI 信息到指定文件的名称，1～32 个字符的字符串，不区分大小写，且不能包含如下字符：\ / : * ? " < > |。

【使用指导】

export oui 命令用来导出所有的 OUI 信息到指定的文件，包括 WIPS 系统 OUI 库中的 OUI 信息和导入的配置文件中的 OUI 信息。

导出文件格式如下：

```
000FE2     (base 16)        New H3C Technologies Co., Ltd..
```

【举例】

导出所有的 OUI 信息到文件 OUIInfo 中。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] export oui OUIInfo
```

【相关命令】

- **import oui**
- **reset wips embedded-oui**

1.1.63 flood association-request

flood association-request 命令用来开启关联请求帧泛洪攻击检测功能。

undo flood association-request 命令用来关闭关联请求帧泛洪攻击检测功能。

【命令】

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

【缺省情况】

关联请求帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测关联请求帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60 秒。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600 秒。在静默期间，设备在统计周期内收到的关联请求帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测关联请求帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的关联请求帧达到触发阈值，即判定设备受到关联请求帧泛洪攻击，设备会发送告警信息。

【举例】

开启关联请求帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360
```

1.1.64 flood authentication

flood authentication 命令用来开启认证请求帧泛洪攻击检测功能。

undo flood authentication 命令用来关闭认证请求帧泛洪攻击检测功能。

【命令】

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

【缺省情况】

认证请求帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测认证请求帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60 秒。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600 秒。在静默期间，设备在统计周期内收到的认证请求帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测认证请求帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的认证请求帧达到触发阈值，即判定设备受到认证请求帧泛洪攻击，设备会发送告警信息。

【举例】

开启认证请求帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360
```

1.1.65 flood beacon

flood beacon 命令用来开启 Beacon 帧泛洪攻击检测功能。

undo flood beacon 命令用来关闭 Beacon 帧泛洪攻击检测功能。

【命令】

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

【缺省情况】

Beacon 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 Beacon 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 Beacon 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 Beacon 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 Beacon 帧达到触发阈值，即判定设备受到 Beacon 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 Beacon 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360
```

1.1.66 flood block-ack

flood block-ack 命令用来开启 Block ACK 帧泛洪攻击检测功能。

undo flood block-ack 命令用来关闭 Block ACK 帧泛洪攻击检测功能。

【命令】

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

【缺省情况】

Block ACK 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 Block ACK 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 Block ACK 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 Block ACK 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 Block ACK 帧达到触发阈值，即判定设备受到 Block ACK 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 Block ACK 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360
```

1.1.67 flood cts

flood cts 命令用来开启 CTS 帧泛洪攻击检测功能。

undo flood cts 命令用来关闭 CTS 帧泛洪攻击检测功能。

【命令】

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

【缺省情况】

CTS 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 CTS 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 CTS 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 CTS 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 CTS 帧达到触发阈值，即判定设备受到 CTS 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 CTS 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360
```

1.1.68 flood deauthentication

flood deauthentication 命令用来开启解除认证帧泛洪攻击检测功能。

undo flood deauthentication 命令用来关闭解除认证帧泛洪攻击检测功能。

【命令】

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

【缺省情况】

解除认证帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测解除认证帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的解除认证帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测解除认证帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的解除认证帧达到触发阈值，即判定设备受到解除认证帧泛洪攻击，设备会发送告警信息。

【举例】

#开启解除认证帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360
```

1.1.69 flood disassociation

flood disassociation 命令用来开启解除关联帧泛洪攻击检测功能。

undo flood disassociation 命令用来关闭解除关联帧泛洪攻击检测功能。

【命令】

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

【缺省情况】

解除关联帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测解除关联帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的解除关联帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测解除关联帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的解除关联帧达到触发阈值，即判定设备受到解除关联帧泛洪攻击，设备会发送告警信息。

【举例】

开启解除关联帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360
```

1.1.70 flood eap-failure

flood eap-failure 命令用来开启 EAP-Failure 帧泛洪攻击检测功能。

undo flood eap-failure 命令用来关闭 EAP-Failure 帧泛洪攻击检测功能。

【命令】

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

【缺省情况】

EAP-Failure 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 EAP-Failure 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的 EAP-Failure 帧的数量达到触发告警阈值，也不会发送告警日志。

threshold *threshold-value*：检测 EAP-Failure 帧的数量达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 EAP-Failure 帧的数量达到触发告警阈值，即判定设备受到 EAP-Failure 帧泛洪攻击，设备会发送告警日志。

【举例】

开启 EAP-Failure 帧的泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360
```

1.1.71 flood eap-success

flood eap-success 命令用来开启 EAP-Success 帧泛洪攻击检测功能。

undo flood eap-success 命令用来关闭 EAP-Success 帧泛洪攻击检测功能。

【命令】

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

【缺省情况】

EAP-Success 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 EAP-Success 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的 EAP-Success 帧的数量达到触发告警阈值，也不会发送告警日志。

threshold *threshold-value*：检测 EAP-Success 帧的数量达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 EAP-Success 帧达到触发告警阈值，即判定设备受到 EAP-Success 帧泛洪攻击，设备会发送告警日志。

【举例】

开启 EAP-Success 帧的泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
```

```
[Sysname-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360
```

1.1.72 flood eapol-logoff

flood eapol-logoff 命令用来开启 EAPOL-Logoff 帧泛洪攻击检测功能。

undo flood eapol-logoff 命令用来关闭 EAPOL-Logoff 帧泛洪攻击检测功能。

【命令】

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

【缺省情况】

EAPOL-Logoff 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 EAPOL-Logoff 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在统计周期内检测到的 EAPOL-Logoff 帧的数量达到触发告警阈值，也不会发送告警日志。

threshold *threshold-value*：检测 EAPOL-Logoff 帧达到触发告警阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 EAPOL-Logoff 帧的数量达到触发告警阈值，即判定设备受到 EAPOL-Logoff 帧泛洪攻击，设备会发送告警日志。

【举例】

开启 EAPOL-Logoff 帧的泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360
```

1.1.73 flood eapol-start

flood eapol-start 命令用来开启 EAPOL-Start 帧泛洪攻击检测功能。

undo flood eapol-start 命令用来关闭 EAPOL-Start 帧泛洪攻击检测功能。

【命令】

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

【缺省情况】

EAPOL-Start 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 EAPOL-Start 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 EAPOL-Start 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 EAPOL-Start 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 EAPOL-Start 帧达到触发阈值，即判定设备受到 EAPOL-Start 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 EAPOL-Start 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360
```

1.1.74 flood null-data

flood null-data 命令用来开启 Null data 帧泛洪攻击检测功能。

undo flood null-data 命令用来关闭 Null data 帧泛洪攻击检测功能。

【命令】

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

【缺省情况】

Null data 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 Null data 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 Null data 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 Null data 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 Null data 帧达到触发阈值，即判定设备受到 Null data 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 Null data 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360
```

1.1.75 flood probe-request

flood probe-request 命令用来开启探查请求帧泛洪攻击检测功能。

undo flood probe-request 命令用来关闭探查请求帧泛洪攻击检测功能。

【命令】

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

【缺省情况】

探查请求帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测探查请求帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的探查请求帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测探查请求帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的探查请求帧达到触发阈值，即判定设备受到探查请求帧泛洪攻击，设备会发送告警信息。

【举例】

开启探查请求帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360
```

1.1.76 flood reassociation-request

flood reassociation-request 命令用来开启重关联帧泛洪攻击检测功能。

undo flood reassociation-request 命令用来关闭重关联帧泛洪攻击检测功能。

【命令】

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

【缺省情况】

重关联帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测重关联帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的重关联帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测重关联帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的重关联帧达到触发阈值，即判定设备受到重关联帧泛洪攻击，设备会发送告警信息。

【举例】

开启重关联帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360
```

1.1.77 flood rts

flood rts 命令用来开启 RTS 帧泛洪攻击检测功能。

undo flood rts 命令用来关闭 RTS 帧泛洪攻击检测功能。

【命令】

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

【缺省情况】

RTS 帧泛洪攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测 RTS 帧的统计周期，取值范围为 1～3600，单位为秒，缺省值为 60。

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备在统计周期内收到的 RTS 帧即使达到触发告警阈值，设备也不会发送告警信息。

threshold *threshold-value*：检测 RTS 帧达到触发阈值，取值范围为 1～100000，缺省值为 50。当设备在一个统计周期内检测到的 RTS 帧达到触发阈值，即判定设备受到 RTS 帧泛洪攻击，设备会发送告警信息。

【举例】

开启 RTS 帧泛洪攻击检测功能，统计周期为 100 秒，触发告警阈值为 100，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360
```

1.1.78 frame-type

frame-type 命令用来配置 Signature 规则中匹配帧类型的子规则。

undo frame-type 命令用来恢复缺省情况。

【命令】

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

【缺省情况】

未配置 Signature 规则中匹配帧类型的子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

control：控制帧。

data：数据帧。

management：管理帧。

frame-subtype：帧的子类型。

association-request：Association Request 帧。

association-response：Association Response 帧。

authentication：Authentication 帧。

beacon：Beacon 帧。

deauthentication：De-authentication 帧。

disassociation：Disassociation 帧。

probe-request：Probe Request 帧。

【举例】

配置 ID 为 1 的 Signature 规则中帧类型为数据帧的匹配子规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[wips-sig-rule-1] frame-type data
```

【相关命令】

- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid(signature rule view)**
- **pattern**
- **match all(signature rule view)**

1.1.79 honeypot-ap

honeypot-ap 命令用来开启蜜罐 AP 检测功能。

undo honeypot-ap 命令用来关闭蜜罐 AP 检测功能。

【命令】

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

【缺省情况】

蜜罐 AP 检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

similarity *similarity-value*：SSID 的相似度，取值范围为 70～100，缺省值为 80。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到蜜罐 AP，设备也不会发送告警日志。

【举例】

开启蜜罐 AP 检测功能，SSID 相似度为 90%，静默时间为 10 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] honeypot-ap similarity 90 quiet 10
```

1.1.80 hotspot-attack

hotspot-attack 命令用来开启热点攻击检测功能。

undo hotspot-attack 命令用来关闭热点攻击检测功能。

【命令】

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

【缺省情况】

热点攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备检测到热点攻击，设备也不会发送告警日志。

【举例】

开启热点攻击检测功能，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
```

```
[Sysname-wips-dtc-home] hotspot-attack quiet 100
```

【相关命令】

- **import hotspot**

1.1.81 ht-40mhz-intolerance

ht-40mhz-intolerance 命令用来开启客户端是否开启了禁用 802.11n 40MHz 模式检测功能。

undo ht-40mhz-intolerance 命令用来关闭客户端是否开启了禁用 802.11n 40MHz 模式检测功能。

【命令】

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-40mhz-intolerance

【缺省情况】

客户端是否开启了禁用 802.11n 40MHz 模式检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到客户端开启了禁用 802.11n 40MHz 模式，也不会发送告警日志。

【举例】

开启客户端是开启了否禁用 802.11n 40MHz 模式检测功能，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ht-40mhz-intolerance quiet 100
```

1.1.82 ht-greenfield

ht-greenfield 命令用来开启绿野模式检测功能。

undo ht-greenfield 命令用来关闭绿野模式检测功能。

【命令】

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

【缺省情况】

绿野模式检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到 AP 工作在绿野模式，设备也不会发送告警日志。

【举例】

开启绿野模式检测功能，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] ht-greenfield quiet 100
```

1.1.83 ignorelist

ignorelist 命令用来配置忽略 WIPS 告警信息的设备列表。

undo ignorelist 命令用来删除忽略 WIPS 告警信息的设备列表。

【命令】

ignorelist mac-address *mac-address*

undo ignorelist mac-address { *mac-address* | **all** }

【缺省情况】

未配置忽略 WIPS 告警信息的设备列表。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

mac-address：将要忽略 WIPS 告警信息的设备列表中添加或删除的无线设备的 MAC 地址，格式为 H-H-H。

all：删除忽略 WIPS 告警信息的设备列表的所有表项。

【使用指导】

对于忽略 WIPS 告警信息的设备列表中的无线设备，WIPS 会监测其是否存在，但是不会对它的任何行为产生告警。

【举例】

配置 MAC 地址为 2a11-1fa1-1311 的设备加入到忽略告警信息的设备列表中。

```
<Sysname> system-view
[Sysname] wips
```

```
[Sysname-wips] ignorelist mac-address 2a11-1fa1-1311
```

1.1.84 import hotspot

import hotspot 命令用来导入热点信息的配置文件。

undo import hotspot 命令用来删除已导入的热点信息配置文件。

【命令】

import hotspot *file-name*

undo import hotspot

【缺省情况】

未导入热点信息的配置文件。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

file-name：导入配置文件名称，1～255 个字符的字符串，不区分大小写，且文件名不能包含如下字符：\/:*?"<>|。

【使用指导】

最多只能导入一个热点信息的配置文件。

【举例】

导入热点信息的配置文件。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] import hotspot hotspot_cfg
```

【相关命令】

- **hotspot-attack**

1.1.85 import oui

import oui 命令用来导入配置文件中的 OUI 信息。

undo import oui 命令用来恢复缺省情况。

【命令】

import oui *file-name*

undo import oui

【缺省情况】

未导入配置文件的 OUI 信息。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

oui：导入配置文件名称，1～255 个字符的字符串，不区分大小写，且文件名不能包含如下字符：\ / : * ? " < > |。

【使用指导】

- 该配置文件可以从 IEEE 网站下载。
- 最多只能导入一个配置文件。

【举例】

导入配置文件中的 OUI 信息。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] import oui oui_import_cfg
```

【相关命令】

- **export oui**
- **reset wips embedded-oui**

1.1.86 invalid-oui-classify illegal

invalid-oui-classify illegal 命令用来配置对非法 OUI 的设备进行分类。

undo invalid-oui-classify 命令用来恢复缺省情况。

【命令】

invalid-oui-classify illegal

undo invalid-oui-classify

【缺省情况】

不对非法 OUI 的设备进行分类。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【举例】

配置对非法 OUI 的设备进行分类。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] invalid-oui-classify illegal
```

【相关命令】

- **import oui**

1.1.87 mac-address

mac-address 命令用来配置 Signature 规则中匹配报文中携带的 MAC 地址的子规则。

undo mac-address 命令用来恢复缺省情况。

【命令】

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

【缺省情况】

未配置 Signature 规则中匹配报文中携带的 MAC 地址的子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

bssid：对 BSSID 进行匹配。

destination：对目的 MAC 地址进行匹配。

source：对源 MAC 地址进行匹配。

mac-address：指定 MAC 地址，格式为 H-H-H。

【举例】

在编号为 1 的 Signature 规则中配置匹配报文源 MAC 地址为 000f-e201-0101 的子规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[Sysname-wips-sig-rule-1] mac-address source 000f-e201-0101
```

【相关命令】

- **frame-type**
- **seq-number**
- **ssid-length**
- **ssid(signature rule view)**
- **pattern**
- **match all(signature rule view)**

1.1.88 malformed duplicated-ie

malformed duplicated-ie 命令用来开启 IE 重复的畸形报文检测功能。

undo malformed duplicated-ie 命令用来关闭 IE 重复的畸形报文检测功能。

【命令】

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

【缺省情况】

IE 重复的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 IE 重复的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对所有管理帧的检测。当解析某报文时，该报文所包含的某 IE 重复出现时，则判断该报文为重复 IE 畸形报文。因为厂商自定义 IE 是允许重复的，所以检测 IE 重复时，不检测厂商自定义 IE。

【举例】

开启 IE 重复的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed duplicated-ie quiet 360
```

1.1.89 malformed fata-jack

malformed fata-jack 命令用来开启 Fata-Jack 畸形报文检测功能。

undo malformed fata-jack 命令用来关闭 Fata-Jack 畸形报文检测功能。

【命令】

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

【缺省情况】

Fata-Jack 畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 Fata-Jack 畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对认证帧的检测。Fata-Jack 畸形类型规定，当身份认证算法编号即 Authentication algorithm number 的值等于 2 时，则判定该帧为 Fata-Jack 畸形报文。

【举例】

开启 Fata-Jack 畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed fata-jack quiet 360
```

1.1.90 malformed illegal-ibss-ess

malformed illegal-ibss-ess 命令用开启 IBSS 和 ESS 置位异常的畸形报文检测功能。

undo malformed illegal-ibss-ess 命令用来关闭 IBSS 和 ESS 置位异常的畸形报文检测功能。

【命令】

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

【缺省情况】

IBSS 和 ESS 置位异常的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 IBSS 和 ESS 置位异常的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对 Beacon 帧和探查响应帧进行的检测。当报文中的 IBSS 和 ESS 都置位为 1 时，由于此种情况在协议中没有定义，所以这类报文被判定为 IBSS 和 ESS 置位异常的畸形报文。

【举例】

开启 IBSS 和 ESS 置位异常的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed illegal-ibss-ess quiet 360
```

1.1.91 malformed invalid-address-combination

malformed invalid-address-combination 命令用来开启源地址为广播或者组播的认证和关联畸形报文检测功能。

undo malformed invalid-address-combination 命令用来关闭源地址为广播或者组播的认证和关联畸形报文检测功能。

【命令】

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

【缺省情况】

源地址为广播或者组播的认证和关联畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到报文长度非法的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对所有管理帧的检测。当检测到该帧的 TO DS 等于 1 时，表明该帧为客户端发给 AP 的，如果同时又检测到该帧的源 MAC 地址为广播或组播，则该帧被判定为 Invalid-source-address 畸形报文。

【举例】

开启源地址为广播或者组播的认证和关联畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-address-combination quiet 360
```

1.1.92 malformed invalid-assoc-req

malformed invalid-assoc-req 命令用来开启畸形关联请求报文检测功能。

undo malformed invalid-assoc-req 命令用来关闭畸形关联请求报文检测功能。

【命令】

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

【缺省情况】

畸形关联请求报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到畸形关联请求报文，也不会发送告警信息。

【使用指导】

该检测是针对认证请求帧的检测。当收到认证请求帧中的 SSID 长度等于零时，判定该报文为畸形关联请求报文。

【举例】

开启畸形关联请求报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-assoc-req quiet 360
```

1.1.93 malformed invalid-auth

malformed invalid-auth 命令用来开启畸形认证请求报文检测功能。

undo malformed invalid-auth 命令用来关闭畸形认证请求报文检测功能。

【命令】

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

【缺省情况】

畸形认证请求报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到畸形认证请求报文，也不会发送告警信息。

【使用指导】

该检测是针对认证帧的检测。当检测到以下情况时请求认证过程失败，会被判断判定为认证畸形报文。

- 当对认证帧的身份认证算法编号（Authentication algorithm number）的值不符合协议规定，并且其值大于 3 时；

- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值等于 1，且状态代码 status code 不为零时；
- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值大于 4 时。

【举例】

关闭畸形认证请求报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-auth quiet 360
```

1.1.94 malformed invalid-deauth-code

malformed invalid-deauth-code 命令用来开启含有无效原因值的解除认证畸形报文检测功能。

undo malformed invalid-deauth-code 命令用来关闭含有无效原因值的解除认证畸形报文检测功能。

【命令】

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

【缺省情况】

含有无效原因值的解除认证畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到含有无效原因值的解除认证畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对解除认证畸形帧的检测。当解除认证畸形帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除认证畸形报文。

【举例】

开启含有无效原因值的解除认证畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-deauth-code quiet 360
```

1.1.95 malformed invalid-disassoc-code

malformed invalid-disassoc-code 命令用来开启含有无效原因值的解除关联畸形报文检测功能。

undo malformed invalid-disassoc-code 命令用来关闭含有无效原因值的解除关联畸形报文检测功能。

【命令】

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

【缺省情况】

含有无效原因值的解除关联畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到含有无效原因值的解除关联畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对解除关联帧的检测。当解除关联帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除关联畸形报文。

【举例】

开启含有无效原因值的解除关联畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-disassoc-code quiet 360
```

1.1.96 malformed invalid-ht-ie

malformed invalid-ht-ie 命令用来开启畸形 HT IE 报文检测功能。

undo malformed invalid-ht-ie 命令用来关闭畸形 HT IE 报文检测功能。

【命令】

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

【缺省情况】

畸形 HT IE 报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到畸形 HT IE 报文，也不会发送告警信息。

【使用指导】

该检测是针对 Beacon、探查响应帧、关联响应帧、重关联响应帧的检测。当检测到以下情况时，判定为 HT IE 的畸形报文，发出告警，在静默时间内不再告警。

- 解析出 HT Capabilities IE 的 SM Power Save 值为 2 时；
- 解析出 HT Operation IE 的 Secondary Channel Offset 值等于 2 时。

【举例】

开启畸形 HT IE 报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-ht-ie quiet 360
```

1.1.97 malformed invalid-ie-length

malformed invalid-ie-length 命令用来开启 IE 长度非法的畸形报文检测功能。

undo malformed invalid-ie-length 命令用来关闭 IE 长度非法的畸形报文检测功能。

【命令】

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

【缺省情况】

IE 长度非法的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 IE 长度非法的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对所有管理帧的检测。信息元素（Information Element，简称 IE）是管理帧的组成元件，其长度不定。信息元素通常包含一个元素识别码位（Element ID）、一个长度位（Length）以及一个长度不定的位。每种类型的管理帧包含特定的几种 IE，IE 的长度的取值范围应遵守最新 802.11

协议的规定。报文解析过程中，当检测到该报文包含的某个 IE 的长度为非法时，该报文被判定为 IE 长度非法的畸形报文。

【举例】

开启 IE 长度非法的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-ie-length quiet 360
```

1.1.98 malformed invalid-pkt-length

malformed invalid-pkt-length 命令用来开启报文长度非法的畸形报文检测功能。

undo malformed invalid-pkt-length 命令用来关闭报文长度非法的畸形报文检测功能。

【命令】

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

【缺省情况】

报文长度非法的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到报文长度非法的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对所有管理帧的检测。当解析完报文主体后，IE 的剩余长度不等于零时，则该报文被判定为报文长度非法畸形报文。

【举例】

开启报文长度非法的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed invalid-pkt-length quiet 360
```

1.1.99 malformed large-duration

malformed large-duration 命令用来开启 Duration 字段超大的畸形报文检测功能。

undo malformed large-duration 命令用来关闭 Duration 字段超大的畸形报文检测功能。

【命令】

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

【缺省情况】

Duration 字段超大的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 Duration 字段超大的畸形报文，也不会发送告警信息。

threshold *value*：检测报文中 Duration 字段超大的触发阈值，取值范围为 1～32767，缺省值为 5000。当设备在一个统计周期内检测报文的 Duration 字段达到触发阈值，即判定设备受到 Duration 字段超大的畸形报文，设备会发送告警信息。

【使用指导】

该检测是针对单播管理帧、单播数据帧以及 RTS、CTS、ACK 帧的检测。如果报文解析结果中该报文的 Duration 值大于指定的门限值，则为 Duration 超大的畸形报文。

【举例】

开启 Duration 字段超大的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed large-duration quiet 360
```

1.1.100 malformed null-probe-resp

malformed null-probe-resp 命令用来开启无效探查响应报文检测功能。

undo malformed null-probe-resp 命令用来关闭无效探查响应报文检测功能。

【命令】

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

【缺省情况】

无效探查响应报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到无效探查响应报文，也不会发送告警信息。

【使用指导】

该检测是针对探查响应报文。当检测到该帧为非 Mesh 帧，但同时该帧的 SSID Length 等于零，这种情况不符合协议（协议规定 SSID 等于零的情况是 Mesh 帧），则判定为无效探查响应报文。

【举例】

开启无效探查响应报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed null-probe-resp quiet 360
```

1.1.101 malformed overflow-eapol-key

malformed overflow-eapol-key 命令用来开启 key 长度超长的 EAPOL 报文检测功能。

undo malformed overflow-eapol-key 命令用来关闭 key 长度超长的 EAPOL 报文检测功能。

【命令】

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

【缺省情况】

key 长度超长的 EAPOL 报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 key 长度超长的 EAPOL 报文，也不会发送告警信息。

【使用指导】

该检测是针对 EAPOL-Key 帧的检测。当检测到该帧的 TO DS 等于 1 且其 Key Length 大于零时，则判定该帧为 key 长度超长的 EAPOL 报文。Key length 长度异常的恶意的 EAPOL-Key 帧可能会导致 DOS 攻击。

【举例】

开启 key 长度超长的 EAPOL 报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed overflow-eapol-key quiet 360
```

1.1.102 malformed overflow-ssid

malformed overflow-ssid 命令用来开启 SSID 长度超长的畸形报文检测功能。

undo malformed overflow-ssid 命令用来关闭 SSID 长度超长的畸形报文检测功能。

【命令】

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

【缺省情况】

SSID 长度超长的畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 SSID 长度超长的畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对 Beacon、探查请求、探查响应、关联请求帧的检测。当解析报文的 SSID length 大于 32 字节时，不符合协议规定的 0～32 字节的范围，则判定该帧为 SSID 超长的畸形报文。

【举例】

开启 SSID 长度超长的畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed overflow-ssid quiet 360
```

1.1.103 malformed redundant-ie

malformed redundant-ie 命令用来开启多余 IE 畸形报文检测功能。

undo malformed redundant-ie 命令用来关闭多余 IE 畸形报文检测功能。

【命令】

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

【缺省情况】

多余 IE 畸形报文检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到多余 IE 畸形报文，也不会发送告警信息。

【使用指导】

该检测是针对所有管理帧的检测。报文解析过程中，当遇到既不属于报文应包含的 IE，也不属于 reserved IE 时，判断该 IE 为多余 IE，则该报文被判定为多余 IE 畸形报文。

【举例】

开启多余 IE 畸形报文检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] malformed redundant-ie quiet 360
```

1.1.104 man-in-the-middle

man-in-the-middle 命令用来开启中间人攻击检测功能。

undo man-in-the-middle 命令用来关闭中间人攻击检测功能。

【命令】

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

【缺省情况】

中间人攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到中间人攻击，设备也不会发送告警日志。

【使用指导】

在配置中间人攻击检测之前需要开启蜜罐 AP 检测。

【举例】

开启中间人攻击检测功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] honeypot-ap
```

```
[Sysname-wips-dtc-home] man-in-the-middle
```

1.1.105 manual-classify mac-address

manual-classify mac-address 命令用来将指定的 AP 进行手工分类。

undo manual-classify mac-address 命令用来恢复缺省情况。

【命令】

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

【缺省情况】

没有对 AP 进行手工分类。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【参数】

mac-address：AP 的 MAC 地址，格式为 H-H-H。

authorized-ap：将指定 AP 设置为授权 AP。

external-ap：将指定 AP 设置为外部 AP。

misconfigured-ap：将指定 AP 设置为配置错误的 AP。

rogue-ap：将指定 AP 设置为 Rogue AP。

all：取消对所有 AP 的手工分类。

【举例】

将 MAC 地址为 000f-00e2-0001 的 AP 配置为授权 AP。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap
```

1.1.106 match all(AP classification rule view)

match all 命令用来配置 AP 分类规则的匹配关系为逻辑与。

undo match all 命令用来恢复缺省情况。

【命令】

match all

undo match all

【缺省情况】

AP 分类规则的匹配关系为逻辑或，即 AP 只要符合任何一条匹配条件就匹配上此规则。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【举例】

配置名称为 1 的 AP 分类规则的匹配关系为逻辑与。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] match all
```

1.1.107 match all(signature rule view)

match all 命令用来配置 Signature 规则的匹配子规则的匹配关系为逻辑与。

undo match all 命令用来恢复缺省情况。

【命令】

match all

undo match all

【缺省情况】

Signature 规则的匹配子规则的匹配关系为逻辑或，即只要符合任何一条匹配条件就匹配上此规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【举例】

配置 Signature 规则 1 的匹配子规则的匹配关系为逻辑与。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[wips-sig-rule-1] match all
```

【相关命令】

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid(signature rule view)**
- **pattern**

1.1.108 omerta

omerta 命令用来开启 Omerta 攻击检测功能。

undo omerta 命令用来关闭对 Omerta 攻击的检测功能。

【命令】

omerta [**quiet** *quiet-value*]

undo omerta

【缺省情况】

Omerta 攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到 Omerta 攻击，也不会发送告警日志。

【举例】

开启 Omerta 攻击检测功能，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] omerta quiet 100
```

1.1.109 oui

oui 命令用来在 AP 分类规则中对 AP 设备的 OUI 信息进行匹配。

undo oui 命令用来恢复缺省情况。

【命令】

oui *oui-info*

undo oui

【缺省情况】

没有在 AP 分类规则中对 AP 设备的 OUI 信息进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

oui-info：对 AP 设备进行匹配的 OUI 信息，格式 XXXXXX，16 进制字符串，不区分大小写。

【举例】

在 ID 为 1 的 AP 分类规则中配置 OUI 为 000fe4 的 AP 匹配规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] oui 000fe4
```

1.1.110 pattern

pattern 命令用来配置 Signature 规则中匹配报文中指定位置的字段的子规则。

undo pattern 命令用来恢复缺省情况。

【命令】

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

【缺省情况】

未配置 Signature 规则中匹配报文中指定位置的字段的子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

pattern-number：Signature 规则中匹配报文中指定位置的字段的子规则序列号，取值范围 0~65535。

offset *offset-value*：指定匹配字段相对于参考位置的偏移量，*offset-value* 为偏移量，取值范围为 0～2346，单位为 bit。参考位置可以为帧头部（缺省情况）或帧载荷头部（配置 **from-payload** 参数后）。

mask *mask*：指定用于匹配指定字段的掩码值，*mask* 为十六进制的掩码值，长度为两字节，取值范围为 0～ffff。

value1 [**to** *value2*]：指定匹配条件值的范围。*value1* 和 *value2* 为匹配条件的值，取值范围为 0～65535。*value2* 的值要大于或等于 *value1* 的值。

from-payload：指定偏移量的参考位置为帧载荷的头部。不指定该参数时，偏移量的参考位置为帧头部。

【举例】

在编号为 1 的 Signature 规则中，创建以下匹配规则：匹配从报文头开始第 2、3 两个字节的取值为 0x0015～0x0020 之间的报文。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[Sysname-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20
```

【相关命令】

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid(signature rule view)**
- **match all(signature rule view)**

1.1.111 permit-channel

permit-channel 命令用来配置合法信道集。

undo permit-channel 命令用来删除配置的合法信道集。

【命令】

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

【缺省情况】

未配置合法信道集。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

channel-id-list ：合法信道列表。表示方式为 *channel-id-list* = { *value1* [**to** *value2*] } &<1-10>，取值范围为 1～224，*value2* 的值要大于或等于 *value1* 的值，<1-10> 表示在一条命令中最多可以配置 10 个合法信道或合法信道范围。

all：表示删除所有已配置的合法信道。

【使用指导】

在配置非法信道检测之前请先配置合法信道集，否则所有信道都会被检测为非法信道。

【举例】

设置合法信道为 1。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] permit-channel 1
```

【相关命令】

- **prohibited-channel**

1.1.112 power-save

power-save 命令用来开启节电攻击检测功能。

undo power-save 命令用来关闭节电攻击检测功能。

【命令】

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

【缺省情况】

节电攻击检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：检测节电报文的统计周期，取值范围为 1～3600，单位为秒，缺省值为 10。

minoffpacket *packet-value*：统计周期内检测到最少节电关闭报文的阈值，取值范围为 10～150，单位为个，缺省值为 50。

onoffpercent *percent-value*：检测节电开始报文和节电关闭报文的百分比的阈值，取值范围为 0～100，缺省值为 80。

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备检测到节电攻击，也不会发送告警日志。

【举例】

开启节电攻击检测功能，统计周期为 20 秒，检测最少节电关闭报文的个数为 20，节电开启报文与节电关闭报文的百分比为 90，静默时间为 100。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100
```

1.1.113 prohibited-channel

prohibited-channel 命令用来开启非法信道检测功能。

undo prohibited-channel 命令用来关闭非法信道检测功能。

【命令】

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

【缺省情况】

非法信道检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使设备在非法信道检测到任何帧，也不会发送告警日志。

【使用指导】

在配置非法信道检测之前请先使用 **permit-channel** 命令配置合法信道，否则所有信道都会被检测为非法信道。

【举例】

开启非法信道检测功能，静默时间为 100。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] prohibited-channel quiet 100
```

【相关命令】

- **permit-channel**

1.1.114 random-mac-scan

random-mac-scan enable 命令用来开启随机伪 MAC 地址过滤功能。

undo random-mac-scan enable 命令用来恢复缺省情况。

【命令】

random-mac-scan enable

undo random-mac-scan enable

【缺省情况】

随机伪 MAC 地址过滤功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【举例】

开启随机伪 MAC 地址过滤功能。

```
<Sysname> system-view
[Sysname] wips
```

```
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] random-mac-scan enable
```

1.1.115 report-interval

report-interval 命令用来配置 Sensor 上报检测到的设备信息的时间间隔。

undo report-interval 命令用来恢复缺省情况。

【命令】

report-interval *interval*

undo report-interval

【缺省情况】

Sensor 上报检测到的设备信息的时间间隔为 30000 毫秒。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

interval：Sensor 上报检测到的设备信息的时间间隔，取值范围为 1000～300000，单位为毫秒。

【举例】

配置 Sensor 上报检测到的设备信息的时间间隔为 10000 毫秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] report-interval 10000
```

1.1.116 reset wips embedded-oui

reset wips embedded-oui 命令用来删除 WIPS 系统 OUI 库中所有的内置 OUI 信息。

【命令】

reset wips embedded-oui

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

删除 WIPS 系统 OUI 库的内置 OUI 信息。

```
<Sysname> reset wips embedded-oui
```

【相关命令】

- **export oui**

- **import oui**

1.1.117 reset wips statistics

reset wips statistics 命令用来清除所有 Sensor 上报的信息。

【命令】

reset wips statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除所有 Sensor 上报的信息。

```
<Sysname> reset wips statistics
```

【相关命令】

- **display wips statistics receive**

1.1.118 reset wips virtual-security-domain

reset wips virtual-security-domain 命令用来清除指定 VSD 内学习到的 AP 表项和客户端表项。

【命令】

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

device：虚拟安全域中检测到的设备。

ap：虚拟安全域中检测到的 AP。

all：虚拟安全域中检测到的所有 AP。

mac-address *mac-address*：指定 AP 的 MAC 地址。

client：虚拟安全域中检测到的客户端。

all：虚拟安全域中检测到的所有客户端。

mac-address *mac-address*：指定客户端的 MAC 地址。

all：虚拟安全域中检测到的所有 AP 和客户端。

【举例】

清除 VSD aaa 内学习到的 AP 表项和客户端表项。

```
<Sysname> reset wips virtual-security-domain aaa device all
```

【相关命令】

- **display wips virtual-security-domain device**

1.1.119 reset wips virtual-security-domain countermeasure record

reset wips virtual-security-domain countermeasure record 命令用来清除指定 VSD 内所有被反制过的设备信息。

【命令】

reset wips virtual-security-domain *vsd-name* **countermeasure record**

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

清除指定 VSD 内所有被反制过的设备信息。

```
<Sysname> reset wips virtual-security-domain aaa countermeasure record
```

【相关命令】

- **display wips virtual-security-domain countermeasure record**

1.1.120 rssi-change-threshold

rssi-change-threshold 命令用来配置 WIPS 检测无线设备的信号强度变化阈值。

undo rssi-change-threshold 命令用来恢复缺省情况。

【命令】

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

【缺省情况】

WIPS 检测无线设备的信号强度变化阈值为 20。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

threshold-value：指定 WIPS 检测无线设备的信号强度变化阈值，取值范围为 1～100。

【举例】

配置 WIPS 检测无线设备的信号强度变化阈值为 80。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] rssi-change-threshold 80
```

1.1.121 rssi-threshold

rssi-threshold 命令用来配置 WIPS 根据信号强度对无线设备进行检测。

undo rssi-threshold 命令用来恢复缺省情况。

【命令】

rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

【缺省情况】

未配置 WIPS 根据信号强度对无线设备进行检测。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

ap *ap-rssi-value*：*WIPS* 检测 AP 设备的信号强度阈值，取值范围为 1～100。

client *client-rssi-value*：*WIPS* 检测客户端设备的信号强度阈值，取值范围为 1～100。

【举例】

配置 WIPS 检测信号强度大于 80 的 AP 设备。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] rssi-threshold ap 80
```

1.1.122 rssi

rssi 命令用来在 AP 分类规则中对 AP 信号的信号强度进行匹配。

undo rssi 命令用来恢复缺省情况。

【命令】

rssi *value1* [**to** *value2*]

undo rssi

【缺省情况】

没有在 AP 分类规则中对 AP 信号的信号强度进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

value1 [**to** *value2*]：指定匹配信号强度值的范围。*value1* 和 *value2* 为匹配信号强度值，取值范围为 0～100。*value2* 的值要大于或等于 *value1* 的值。

【举例】

在 ID 为 1 的 AP 分类规则中对信号强度在 20～40 之间的 AP 进行匹配。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] rssi 20 to 40
```

1.1.123 security

security 命令用来在 AP 分类规则中对 AP 使用无线服务的数据安全方式进行匹配。

undo security 命令用来恢复缺省情况。

【命令】

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

【缺省情况】

没有在 AP 分类规则中对 AP 使用无线服务的数据安全方式进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

equal：匹配项与条件相同。

include：匹配项包含条件。

clear：明文方式。

wep：WEP 方式。

wpa：WPA 方式。

wpa2：WPA2 方式。

【举例】

在 ID 为 1 的 AP 分类策略中对采用 WEP 方式接入无线网络的 AP 设备进行匹配。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] security equal wep
```

1.1.124 select sensor all

select sensor all 命令用来开启所有 Sensor 进行反制功能。

undo select sensor all 命令用来关闭所有 Sensor 进行反制功能。

【命令】

select sensor all

undo select sensor all

【缺省情况】

所有 Sensor 进行反制功能处于关闭状态。

【视图】

反制策略视图

【缺省用户角色】

network-admin

【使用指导】

开启所有 sensor 反制功能后，当一个攻击者同时被多个 Sensor 检测到时，所有 Sensor 都会对其进行反制。没有开启该功能时，被最近一次检测到该攻击者的 Sensor 进行反制。

【举例】

开启所有 Sensor 进行反制功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] countermeasure policy home
[Sysname-wips-ctm-home] select sensor all
```

1.1.125 seq-number

seq-number 命令用来配置 Signature 规则中匹配序列号的子规则。

undo seq-number 命令用来恢复缺省情况。

【命令】

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

【缺省情况】

未配置 Signature 规则中匹配序列号的子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

seq-value1 [**to** *seq-value2*]：指定报文序列号的范围。*seq-value1* 和 *seq-value2* 为报文序列号大小，取值范围为 0～4095。*seq-value2* 的值要大于或等于 *seq-value1* 的值。

【举例】

在编号为 1 的 Signature 规则中配置匹配对指定报文序列号为 100 的子规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[wips-sig-rule-1] seq-number 100
```

【相关命令】

- **frame-type**
- **mac-address**
- **ssid-length**
- **ssid(signature rule view)**
- **pattern**
- **match all(signature rule view)**

1.1.126 signature policy

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

undo signature policy 命令用来删除指定的 Signature 策略。

【命令】

signature policy *policy-name*

undo signature policy *policy-name*

【缺省情况】

不存在 Signature 策略。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

创建一个名称为 home 的 Signature 策略，并进入 Signature 策略视图。

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

```
[Sysname] wips
[Sysname-wips] signature policy home
```

1.1.127 signature rule

signature rule 命令用来创建 Signature 规则，并进入 Signature 规则视图。如果指定的 Signature 规则已经存在，则直接进入 Signature 规则视图。

undo signature rule 命令用来删除指定的 Signature 规则。

【命令】

signature rule *rule-id*

undo signature rule *rule-id*

【缺省情况】

不存在 Signature 规则。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

rule-id：Signature 规则的编号，取值范围为 1～65535。

【举例】

创建编号为 1 的 Signature 规则，并进入 Signature 规则视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
```

1.1.128 soft-ap

soft-ap 命令用来开启软 AP 检测功能。

undo soft-ap 命令用来关闭软 AP 检测功能。

【命令】

soft-ap [**convert-time** *time-value*]

undo soft-ap

【缺省情况】

软 AP 检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

convert-time *time-value*：配置判定设备为软 AP 的角色切换周期，即如果某个 MAC 地址在指定的时间间隔内在无线客户端与 AP 两个角色之间发生切换，则认定该设备为软 AP。*time-value* 为时间间隔，取值范围 5～600，单位为秒，缺省取值为 10。

【举例】

开启软 AP 检测功能，判断软 AP 的依据为设备在 100 秒内发生角色切换。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] soft-ap convert-time 100
```

1.1.129 ssid (AP classification rule view)

ssid 命令用来在 AP 分类规则中对 AP 使用无线服务的 SSID 进行匹配。

undo ssid 命令用来恢复缺省情况。

【命令】

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

【缺省情况】

没有在 AP 分类规则中对 AP 使用无线服务的 SSID 进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

case-sensitive：与 SSID 匹配时需要按照字母的大小写匹配。

not：匹配项与条件不等于或者不包括。

equal：匹配项与条件相同。

include：匹配项包含条件。

ssid-string：与 SSID 进行匹配的字符串，为 1～32 个字符的字符串，区分大小写。

【举例】

在 ID 为 1 的 AP 分类策略中匹配 SSID 为 abc 的 AP。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] ssid equal abc
```

1.1.130 ssid(signature rule view)

ssid 命令用来配置 Signature 规则中匹配 SSID 的子规则。

undo ssid 命令用来恢复缺省情况。

【命令】

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

【缺省情况】

未配置 Signature 规则中匹配 SSID 的子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

case-sensitive：与 SSID 匹配时需要按照字母的大小写匹配。

not：匹配项与条件不等于或不包括。

equal：匹配项与条件相同。

include：匹配项包含条件。

string：与 SSID 进行匹配的字符串，为 1～32 个字符的字符串，区分大小写。

【举例】

配置 ID 为 1 的 Signature 规则中 SSID 等于 office 的匹配子规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[Sysname-wips-sig-rule-1] ssid equal office
```

【相关命令】

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **pattern**
- **match all(signature rule view)**

1.1.131 ssid-length

ssid-length 命令用来配置 Signature 规则中 SSID 长度的匹配子规则。

undo ssid-length 命令用来恢复缺省情况。

【命令】

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

【缺省情况】

未配置 Signature 规则中 SSID 长度的匹配子规则。

【视图】

Signature 规则视图

【缺省用户角色】

network-admin

【参数】

length-value1 [**to** *length-value2*]：指定 SSID 长度的范围。*length-value1* 和 *length-value2* 为 SSID 长度，取值范围为 1～32。*length-value2* 的值要大于或等于 *length-value1* 的值。

【举例】

配置 ID 为 1 的 Signature 规则中 SSID 长度为 10 的匹配子规则。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] signature rule 1
[Sysname-wips-sig-1] ssid-length 10
```

【相关命令】

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid(signature rule view)**
- **pattern**
- **match all(signature rule view)**

1.1.132 trust mac-address

trust mac-address 命令用来将指定的 MAC 地址添加到信任设备列表中。

undo trust mac-address 命令用来删除信任设备列表中的 MAC 地址。

【命令】

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

【缺省情况】

信任设备列表中不存在 MAC 地址。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【参数】

mac-address：AP 或客户端的 MAC 地址。

all：所有 MAC 地址。

【举例】

将 MAC 地址 78AC-C0AF-944F 添加到信任设备列表中。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] trust mac-address 78AC-C0AF-944F
```

1.1.133 trust oui

trust oui 命令用来将指定的 OUI 添加到信任 OUI 列表中。

undo trust oui 命令用来删除信任 OUI 列表中的 OUI。

【命令】

trust oui *oui*

undo trust oui { *oui* | **all** }

【缺省情况】

信任 OUI 列表中不存在 OUI。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【参数】

oui：OUI 名称，为 6 个字符的字符串，不区分大小写。

all：所有 OUI。

【举例】

将名为 000fe4、000fe5 的 OUI 添加到信任 OUI 列表中。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] trust oui 000fe4
[Sysname-wips-cls-home] trust oui 000fe5
```

1.1.134 trust ssid

trust ssid 命令用来将指定的 SSID 添加到信任设备列表中。

undo trust ssid 命令用来删除信任设备列表中的 SSID。

【命令】

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

【缺省情况】

信任设备列表中不存在 SSID。

【视图】

分类策略视图

【缺省用户角色】

network-admin

【参数】

ssid-name：SSID 的名称，为 1～32 个字符的字符串，区分大小写。

all：所有 SSID。

【举例】

将名为 flood1 的 SSID 添加到信任设备列表中。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] classification policy home
[Sysname-wips-cls-home] trust ssid flood1
```

1.1.135 unencrypted-authorized-ap

unencrypted-authorized-ap 命令用来开启未加密授权 AP 检测功能。

undo unencrypted-authorized-ap 命令用来关闭对未加密授权 AP 的检测功能。

【命令】

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

【缺省情况】

未加密授权 AP 检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。

【举例】

开启未加密授权的 AP 检测功能，静默时间为 10 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
```

```
[Sysname-wips-dtc-home] unencrypted-authorized-ap quiet 10
```

1.1.136 unencrypted-trust-client

unencrypted-trust-client 命令用来开启未加密的信任客户端检测功能。

undo unencrypted-trust-client 命令用来关闭未加密的信任客户端检测功能。

【命令】

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

【缺省情况】

未加密的信任客户端检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。

【举例】

开启未加密的信任客户端检测功能，静默时间为 10 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] unencrypted-trust-client quiet 10
```

1.1.137 up-duration

up-duration 命令用来在 AP 分类规则中对 AP 的运行时间进行匹配。

undo up-duration 命令用来恢复缺省情况。

【命令】

up-duration *value1* [**to** *value2*]

undo up-duration

【缺省情况】

没有在 AP 分类规则中对 AP 的运行时间进行匹配。

【视图】

AP 分类规则视图

【缺省用户角色】

network-admin

【参数】

value1 [**to** *value2*]：指定匹配运行时间条件值的范围。*value1* 和 *value2* 为匹配运行时间条件值，取值范围为 0～2592000，单位为秒。*value2* 的值要大于或等于 *value1* 的值。

【举例】

在 ID 为 1 的 AP 分类规则中配置匹配运行时间在 2000～40000 秒之间的 AP。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] ap-classification rule 1
[Sysname-wips-cls-rule-1] up-duration 2000 to 40000
```

1.1.138 virtual-security-domain

virtual-security-domain 命令用来创建 VSD（Virtual Security Domain，虚拟安全域），并进入 VSD 视图，如果指定的 VSD 已经存在，则直接进入 VSD 视图。

undo virtual-security-domain 命令用来删除已创建的 VSD。

【命令】

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

【缺省情况】

不存在 VSD。

【视图】

WIPS 视图

【缺省用户角色】

network-admin

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

创建名称为 office 的 VSD，并进入 VSD 视图。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] virtual-security-domain office
[Sysname-wips-vsd-office]
```

1.1.139 weak-iv

weak-iv 命令用来开启 Weak IV 检测功能。

undo weak-iv 命令用来关闭 Weak IV 检测功能。

【命令】

weak-iv [**quiet** *quiet-value*]

undo weak-iv

【缺省情况】

Weak IV 检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警信息后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备再次检测到 Weak IV 也不会发送告警信息。

【使用指导】

设备检测到 Weak IV 后会发送告警信息。

【举例】

开启 Weak IV 检测功能。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] weak-iv
```

1.1.140 windows-bridge

windows-bridge 命令用来开启 Windows 网桥检测功能。

undo windows-bridge 命令用来关闭 Windows 网桥检测功能。

【命令】

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

【缺省情况】

Windows 网桥检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，设备检测到 Windows 网桥，设备也不会发送告警日志。

【举例】

开启 Windows 网桥检测功能，静默时间为 360 秒。

```
<Sysname> system-view
[Sysname] wips
```

```
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] windows-bridge quiet 360
```

1.1.141 wips (Radio view)

wips enable 命令用来开启 WIPS 功能。

wips disable 命令用来关闭 WIPS 功能。

undo wips 命令用来恢复缺省情况。

【命令】

wips { **disable** | **enable** }

undo wips

【缺省情况】

WIPS 功能处于关闭状态。

【视图】

Radio 接口视图

【缺省用户角色】

network-admin

【举例】

开启 WIPS 功能。

```
<Sysname> system-view
[Sysname] interface wlan-radio 1/0/1
[Sysname-wlan-radio-1] wips enable
```

1.1.142 wips (System view)

wips 命令用来进入 WIPS 视图。

undo wips 命令用来删除 WIPS 视图下所有配置。

【命令】

wips

undo wips

【缺省情况】

未配置 WIPS 视图。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

进入 WIPS 视图。

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

```
[Sysname] wips
[Sysname-wips]
```

1.1.143 wips virtual-security-domain

wips virtual-security-domain 命令用来将 AP 加入到指定的 VSD 中。

undo wips virtual-security-domain 命令用来删除已加入 VSD 的 AP。

【命令】

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

【缺省情况】

没有将 AP 加入到任何的 VSD 中。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vsd-name：虚拟安全域的名称，为 1～63 个字符的字符串，区分大小写。

【举例】

将 AP 加入到名为 office 的 VSD 中。

```
<Sysname> system-view
[Sysname] wips virtual-security-domain office
```

1.1.144 wireless-bridge

wireless-bridge 命令用来开启无线网桥检测功能。

undo wireless-bridge 命令用来关闭无线网桥检测功能。

【命令】

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

【缺省情况】

无线网桥检测功能处于关闭状态。

【视图】

攻击检测策略视图

【缺省用户角色】

network-admin

【参数】

quiet *quiet-value*：发送告警日志后的静默时间，取值范围为 5～604800，单位为秒，缺省值为 600。在静默期间，即使检测到无线网桥，设备也不会发送告警日志。

【举例】

开启无线网桥检测功能，静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] wips
[Sysname-wips] detect policy home
[Sysname-wips-dtc-home] wireless-bridge quiet 100
```