H3C 无线控制器

WIPS 针对所有 SSID 进行反制典型配置举例（V7）

资料版本：6W100-20191125

目 录

1 简介

本文档介绍了 WIPS 针对所有 SSID 进行反制典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

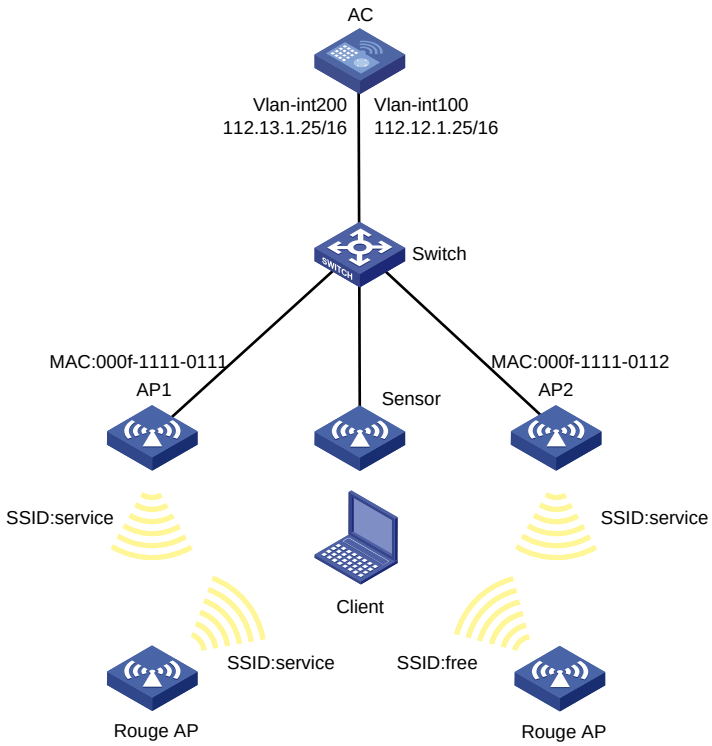
本文档假设您已了解 WIPS 特性。

3 配置举例

3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，AP1 和 AP2 为 Client 提供无线服务，配置 SSID 为 service，在 Sensor 上开启 WIPS 功能，当检测到非法 AP 提供非法的 SSID（service 或其他任意 SSID 比如 free）提供给 Client 接入时，这时 Sensor AP 对非法 AP 会进行反制，阻止 Client 在非法 AP 上线。

图1 WIPS 针对所有 SSID 进行反制配置组网图



3.2 配置步骤

3.2.1 配置AC

(1) 配置 AC 的接口

创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AP 将通过该 IP 地址与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IP 地址。Client 使用 VLAN200 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 200 通过，PVID 为 100。

```
[AC] interface gigabitethernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置 DHCP server

开启 DHCP server 功能。

```
[AC] dhcp enable
```

配置 DHCP 地址池 vlan100 为 AP 分配地址范围为 112.12.0.0/16，网关地址为 112.12.1.25。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

配置 DHCP 地址池 vlan200 为 Client 分配地址范围为 112.13.0.0/16，为 Client 分配的 DNS 服务器地址为网关地址（实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址），网关地址为 112.13.1.25。

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

(3) 配置 WIPS

进入 WIPS 视图。

```
[AC] wips
```

配置 AP 分类规则，对 SSID 为 service 的进行匹配。

```
[AC-wips] ap-classification rule 1
[AC-wips-cls-rule-1] ssid equal service
[AC-wips-cls-rule-1] quit
```

配置 AP 分类规则，对 SSID 不为 service 的进行匹配。

```
[AC-wips] ap-classification rule 2
[AC-wips-cls-rule-2] ssid not equal service
[AC-wips-cls-rule-2] quit
```

配置 AP 分类策略，对符合分类规则 rule1 和 rule2 的 AP 分类为非法 AP，设置反制的优先级为最高，并将 AP1 和 AP2 加入到信任列表中。

```
[AC-wips] classification policy class1
[AC-wips-cls-class1] apply ap-classification rule 1 rogue-ap severity-level 100
[AC-wips-cls-class1] apply ap-classification rule 2 rogue-ap severity-level 100
[AC-wips-cls-class1] trust mac-address 000f-1111-0111
[AC-wips-cls-class1] trust mac-address 000f-1111-0112
[AC-wips-cls-class1] quit
```

创建虚拟安全域，并应用分类策略到虚拟安全域 vsd1。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-1] apply classification policy class1
[AC-wips-vsd-1] quit
```

配制反制策略，反制非法 AP。

```
[AC-wips] countermeasure policy 1
[AC-wips-cms-1] countermeasure rogue-ap
[AC-wips-cms-1] quit
```

应用反制策略到虚拟安全域 vsd1。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply countermeasure policy 1
[AC-wips-vsd-vsd1] quit
[AC-wips] quit
```

(4) 配置 AP

创建无线服务模板 service，并配置 SSID 为 service，配置 Client 从无线服务模板 service 上线后会被加入 VLAN 200，并开启服务模板。

```
[AC] wlan service-template service
[AC-wlan-st-service] ssid service
[AC-wlan-st-service] vlan 200
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

创建手工 AP，名称为 ap1，选择 AP 型号并配置序列号，将无线服务模板绑定到射频接口。

```
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] serial-id 210235A1GQC157001570
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
```

```
[AC-wlan-ap-ap1-radio-1] quit
```
创建手工 AP，名称为 ap2，选择 AP 型号并配置序列号，将无线服务模板绑定到射频接口。
```
[AC] wlan ap ap2 model WA4320i-ACN
[AC-wlan-ap-ap2] serial-id 210235A1GQC157001571
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] service-template service
[AC-wlan-ap-ap2-radio-1] quit
```
创建手工 AP，名称为 sensor，选择 AP 型号并配置序列号，在射频接口开启 WIPS 功能并加入虚拟安全域中。
```
[AC] wlan ap sensor model WA4320i-ACN
[AC-wlan-ap-sensor] serial-id 210235A1GQC157001572
[AC-wlan-ap-sensor] radio 1
[AC-wlan-ap-sensor-radio-1] radio enable
[AC-wlan-ap-sensor-radio-1] wips enable
[AC-wlan-ap-sensor-radio-1] quit
[AC-wlan-ap-sensor] radio 2
[AC-wlan-ap-sensor-radio-2] radio enable
[AC-wlan-ap-sensor-radio-2] wips enable
[AC-wlan-ap-sensor-radio-2] quit
[AC-wlan-ap-sensor] wips virtual-security-domain vsd1
[AC-wlan-ap-sensor] return
```

3.2.2 配置Switch

创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 CAPWAP 隧道内的流量，VLAN 200 用于转发 Client 无线报文。
```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```
配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，禁止 VLAN 1 报文通过，允许 VLAN 100 和 200 通过，PVID 为 100。
```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```
配置 Switch 与 Sensor 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。
```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```
开启 PoE 接口远程供电功能。
```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

配置 Switch 与 AP1 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

开启 PoE 接口远程供电功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

配置 Switch 与 AP2 相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

开启 PoE 接口远程供电功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

3.3 验证配置

(1) 查看 Sensor 所在虚拟安全域扫描到的设备，Rogue AP 提供的服务 SSID 和本地 AC 关联的业务 AP 提供的服务 SSID 相同，WIPS 能正确识别关联的业务 AP 为授权 AP，Rogue AP 为非法 AP。

```
<AC> display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1

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

MAC address  Type  Class   Duration    Sensors Channel Status
000f-1111-0111 AP   Auth   00h 05m 26s 1       161     Active
000f-1111-0112 AP   Auth   00h 05m 26s 1       161     Active
000f-e200-1202 AP   Rogue  00h 05m 26s 1       161     Active
000f-e200-1222 AP   Rogue  00h 05m 26s 1       161     Active
```

可以查看到外部 AP 被分类成 Rogue AP，正确关联的 AP 被分类成授权 AP。

(2) 验证反制功能正常，通过 **display wips virtual-security-domain vsd1 countermeasure record** 命令查看反制记录。

```
<AC> display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in
virtual-security-domain vsd1

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

MAC address    Type   Reason   Countermeasure AP      Radio ID  Time
000f-e200-1202 AP     Class    sensor                 1         2019-09-20/07:20:38
000f-e200-1222 AP     Class    sensor                 1         2019-09-20/07:20:38
```

3.4 配置文件

- AC：

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 gateway-list 112.12.1.25
 network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
 gateway-list 112.13.1.25
 network 112.13.0.0 mask 255.255.0.0
 dns-list 112.13.1.25
#
wlan service-template service
 ssid service
 vlan 200
 service-template enable
#
interface Vlan-interface100
 ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
wlan ap ap1 model WA4320i-ACN
 serial-id 210235A1GQC157001570
 radio 1
  radio enable
  service-template service
#
wlan ap ap2 model WA4320i-ACN
 serial-id 210235A1GQC157001571
 radio 1
  radio enable
  service-template service
#
```

```
wlan ap sensor model WA4320i-ACN
 serial-id 210235A1GQC157001572
 wips virtual-security-domain vsd1
 radio 1
  radio enable
  wips enable
#
wips
 #
 ap-classification rule 1
  ssid equal service
#
 ap-classification rule 2
  ssid not equal service
 #
 classification policy class1
  apply ap-classification rule 1 rogue-ap severity-level 100
  apply ap-classification rule 2 rogue-ap severity-level 100
  trust mac-address 000f-1111-0111
  trust mac-address 000f-1111-0112

 #
 countermeasure policy 1
  countermeasure rogue-ap
 #
 virtual-security-domain vsd1
  apply classification policy class1
  apply countermeasure policy 1
#
```

- Switch：

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
 port access vlan 100
poe enable
```

```
#
interface GigabitEthernet1/0/4
 port access vlan 100
poe enable
#
```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 安全命令参考”。