H3C无线控制器WIPS典型配置举例(V7)

wlan接入 wlan安全 攻击检测及防范 **李晨光** 2016-07-07 发表

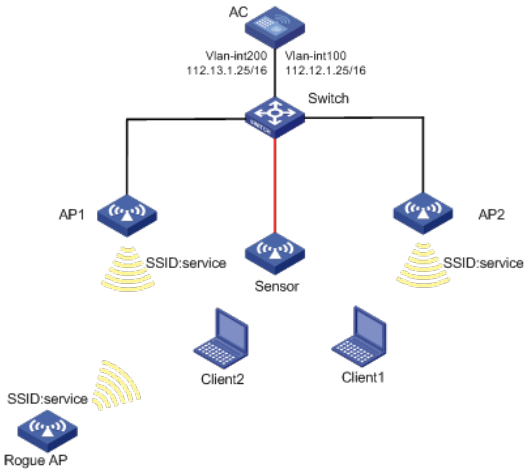
本文档介绍了无线控制器WIPS特性的典型配置举例。

本文档适用于使用Comware V7软件版本的无线控制器和接入点产品，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。

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SSID为service诱使Client接入时，对非法AP进行反制，阻止Client在非法AP上线。



1.1 配置思路

把提供SSID为“service”无线服务的AP分类为Rogue AP，配置Rogue AP反制，因为关联AP分类优先级高于自定义分类，因此提供SSID为“service”无线服务的关联AP依旧会被分类为授权AP。

1.2 配置步骤

1.2.1 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。

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，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] quit

(3) 配置WIPS

进入WIPS视图。

[AC] wips

配置AP分类规则，对无线服务的SSID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分类策略，对符合分类规则rule1的AP分类为非法AP。

[AC-wips] classification policy class1

[AC-wips-cls-class1] apply ap-classification rule 1 rogue-ap

[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

配置反制策略，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] wips virtual-security-domain vsd1

[AC-wlan-ap-sensor] return

1.2.2 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。

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

[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100

[Switch-GigabitEthernet1/0/1] quit

配置Switch与AP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

1.3 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。

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-1111-0101 AP Auth 00h 05m 24s 1 161 Active

000f-1111-0111 AP Auth 00h 05m 26s 1 13 Active

000f-e200-1202 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**命令查看反制记录。

display wips virtual-security-domain vsd1 countermeasure record

Total 1 times countermeasure, current 1 countermeasure record 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	Sensor name	Radio ID	Time
000f-e200-1202	AP	Rogue	sensor	1	2015-11-27/15:52:53

1.4 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
#
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
```

```
 service-template service
#
wips
 #
 ap-classification rule 1
  ssid equal service
 #
 classification policy class1
  apply ap-classification rule 1 rogue-ap
 #
 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
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#
```

配置AP的序列号时请确保该序列号与AP唯一对应，AP的序列号可以通过AP设备背面的标签获取。