# Instant 入侵检测

入侵检测系统（IDS）用于监测网络中非认证IAP及终端设备，并以日志方式记录这些设备的信息，生成相关报告。

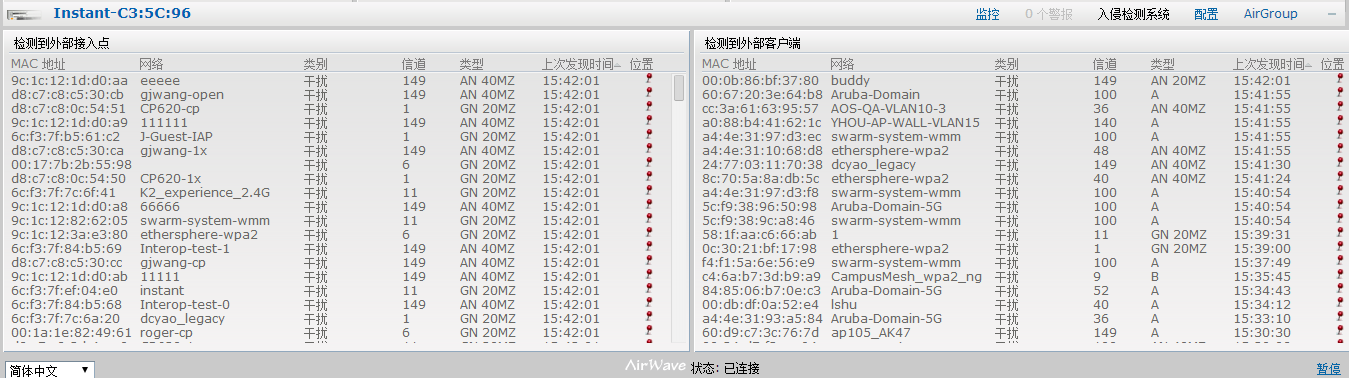
IDS功能在Instant网络中，可以检测非法AP、干扰AP及其他设备，避免产生潜在威胁。

**检测及分类非法AP**

非法AP是未经许可而接入相关有线网络的AP。

干扰AP是释放信号，但未接入相关有线网络的AP。干扰AP可产生潜在的Wifi干扰，降低有效网络利用率。由于并未接入有线交换设备，干扰AP并不会直接对无线网络产生威胁，但也会被定义为非法AP。

为了检测非法AP，在VC的管理页面，点击“入侵检测系统”链接。内置IDS会扫描到未被VC管理的AP。这些AP会根据是否连接到我方网络，而被划分为干扰AP或非法AP。



**终端OS指纹识别**

OS指纹识别功能会收集接入无线网络的终端的信息，并记录该终端的OS类型。以下为该功能的高级应用，

·识别非法终端-找到运行非法OS的终端

·识别过期OS-找到已失去时效的OS，定位该终端位置

·定位并修补不安全OS-协助找到不安全OS的终端，并为该OS打补丁

OS指纹识别在Instant网络中是默认开启的。以下系统可被Instant网络识别，

·Windows 7

·Windows Vista

·Windows Server

·Windows XP

·Windows ME

·OS-X

·iPhone

·iOS

·Android

·Blackberry

·Linux

**配置无线入侵防护及检测基本**

无线入侵防护（WIP）针对无线威胁，提供可选择的检测及保护功能。

与多数Aruba安全保护功能一样，WIP也一样可以在IAP上工作。

你可以配置一下功能：

·基础架构检测策略-针对AP，定义检测无线攻击的策略。

·客户端检测策略-针对客户端，定义检测无线攻击的策略。

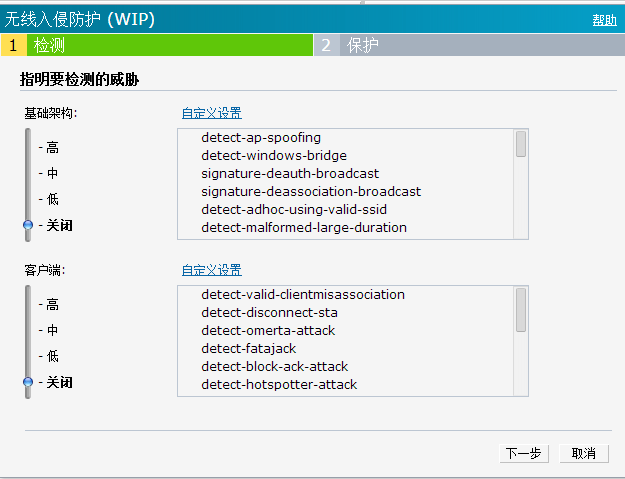
·基础架构保护策略-定义相应保护策略，防止AP受到无线攻击。

·客户端保护策略-定义相应保护策略，防止客户端受到无线攻击。

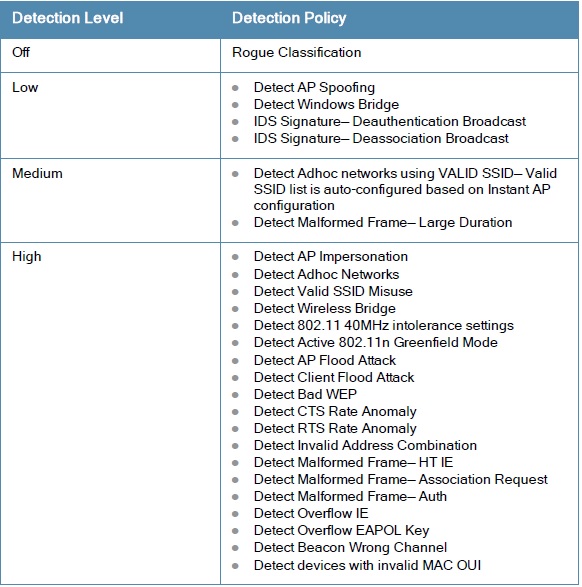
·抑制方法-阻止非授权的客户端接入Instant网络。

每项功能都包含几种不同级别的默认配置。管理员根据实际需要可以启停或编辑各级别配置。

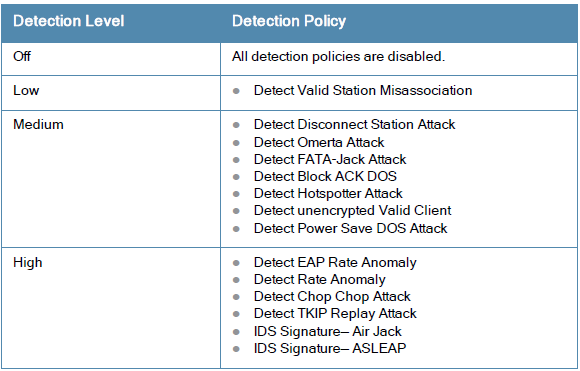
检测策略级别可以在IDS的页面配置。可以点击VC管理主页上的“更多”-“入侵检测系统”查看相关配置。



以下表格描述了基础架构部分不同级别检测策略对应的各项操作，



以下表格描述了客户端检测部分的各项操作，



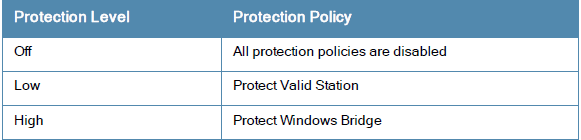
WIP保护部分不同级别策略选择，



基础架构保护部分对应各项操作，



客户端保护部分对应各项操作，



**抑制方法**

通过启用有线和无线抑制，可以组织未授权终端接入Instant网络。

Instant支持以下几种抑制方法，

·有线抑制-启用时，IAP通过ARP方式抑制来自无线网络的攻击

·无线抑制-启用时，系统将尝试断开所有连接中或正在试图连接IAP的客户端。

       ·无-关闭抑制功能。

       ·只解除认证-发送解除认证指令，让无线接口下的AP或客户端断开连接。

       ·阻止电台-AP释放陷阱终端，诱使干扰AP切换信道。



通过命令行配置IDS

(Instant Access Point)(config)# ids

(Instant Access Point)(IDS)# infrastructure-detection-level <type>

(Instant Access Point)(IDS)# client-detection-level <type>

(Instant Access Point)(IDS)# infrastructure-protection-level <type>

(Instant Access Point)(IDS)# client-protection-level <type>

(Instant Access Point)(IDS)# wireless-containment <type>

(Instant Access Point)(IDS)# wired-containment

(Instant Access Point)(IDS)# detect-ap-spoofing

(Instant Access Point)(IDS)# detect-windows-bridge

(Instant Access Point)(IDS)# signature-deauth-broadcast

(Instant Access Point)(IDS)# signature-deassociation-broadcast

(Instant Access Point)(IDS)# detect-adhoc-using-valid-ssid

(Instant Access Point)(IDS)# detect-malformed-large-duration

(Instant Access Point)(IDS)# detect-ap-impersonation

(Instant Access Point)(IDS)# detect-adhoc-network

(Instant Access Point)(IDS)# detect-valid-ssid-misuse

(Instant Access Point)(IDS)# detect-wireless-bridge

(Instant Access Point)(IDS)# detect-ht-40mhz-intolerance

(Instant Access Point)(IDS)# detect-ht-greenfield

(Instant Access Point)(IDS)# detect-ap-flood

(Instant Access Point)(IDS)# detect-client-flood

(Instant Access Point)(IDS)# detect-bad-wep

(Instant Access Point)(IDS)# detect-cts-rate-anomaly

(Instant Access Point)(IDS)# detect-rts-rate-anomaly

(Instant Access Point)(IDS)# detect-invalid-addresscombination

(Instant Access Point)(IDS)# detect-malformed-htie

(Instant Access Point)(IDS)# detect-malformed-assoc-req

(Instant Access Point)(IDS)# detect-malformed-frame-auth

(Instant Access Point)(IDS)# detect-overflow-ie

(Instant Access Point)(IDS)# detect-overflow-eapol-key

(Instant Access Point)(IDS)# detect-beacon-wrong-channel

(Instant Access Point)(IDS)# detect-invalid-mac-oui

(Instant Access Point)(IDS)# detect-valid-clientmisassociation

(Instant Access Point)(IDS)# detect-disconnect-sta

(Instant Access Point)(IDS)# detect-omerta-attack

(Instant Access Point)(IDS)# detect-fatajack

(Instant Access Point)(IDS)# detect-block-ack-attack

(Instant Access Point)(IDS)# detect-hotspotter-attack

(Instant Access Point)(IDS)# detect-unencrypted-valid

(Instant Access Point)(IDS)# detect-power-save-dos-attack

(Instant Access Point)(IDS)# detect-eap-rate-anomaly

(Instant Access Point)(IDS)# detect-rate-anomalies

(Instant Access Point)(IDS)# detect-chopchop-attack

(Instant Access Point)(IDS)# detect-tkip-replay-attack

(Instant Access Point)(IDS)# signature-airjack

(Instant Access Point)(IDS)# signature-asleap

(Instant Access Point)(IDS)# protect-ssid

(Instant Access Point)(IDS)# rogue-containment

(Instant Access Point)(IDS)# protect-adhoc-network

(Instant Access Point)(IDS)# protect-ap-impersonation

(Instant Access Point)(IDS)# protect-valid-sta

(Instant Access Point)(IDS)# protect-windows-bridge

(Instant Access Point)(IDS)# end

(Instant Access Point)# commit apply