目录

简介

思科可适应无线入侵防御系统(wIPS)解决方案添加增强版本地传送方式(榆木)功能，允许管理员使用他们的部署的接入点(AP)提供全面的防护，不用需要对于一个分开的覆盖网络(图1)。在榆木之前和在传统可适应wIPS部署，专用的监控模式(MM) AP要求提供PCI法规遵从性需要或防护从未授权的安全访问、渗透和攻击(图2)。榆木有效提供一可比较提供那缓和无线安全实施，当降低CapEx和OpEx开销时。本文只着重榆木，并且不修改与MM AP的任何现有wIPS部署好处。

图1 -改进的本地传送方式AP部署

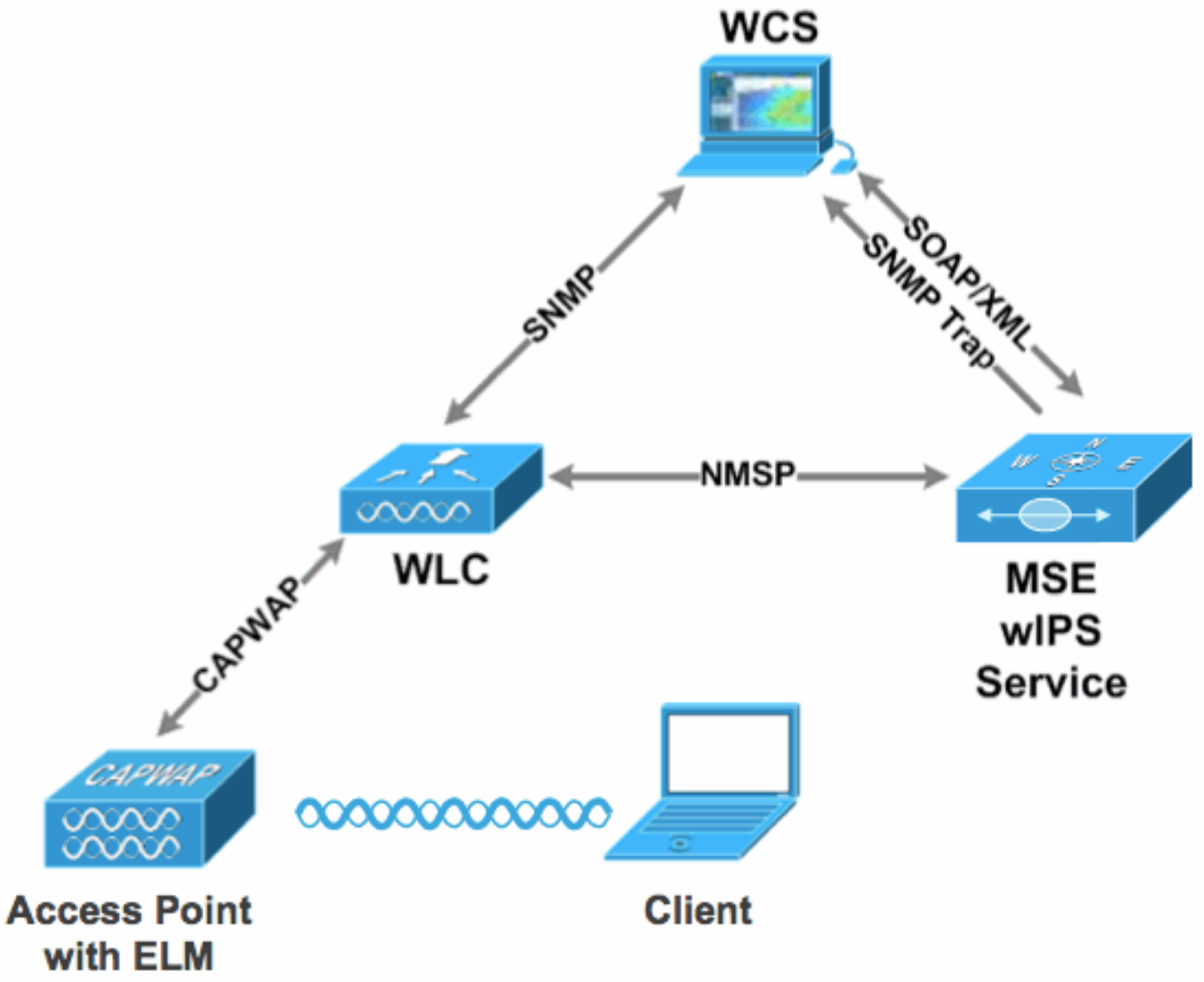
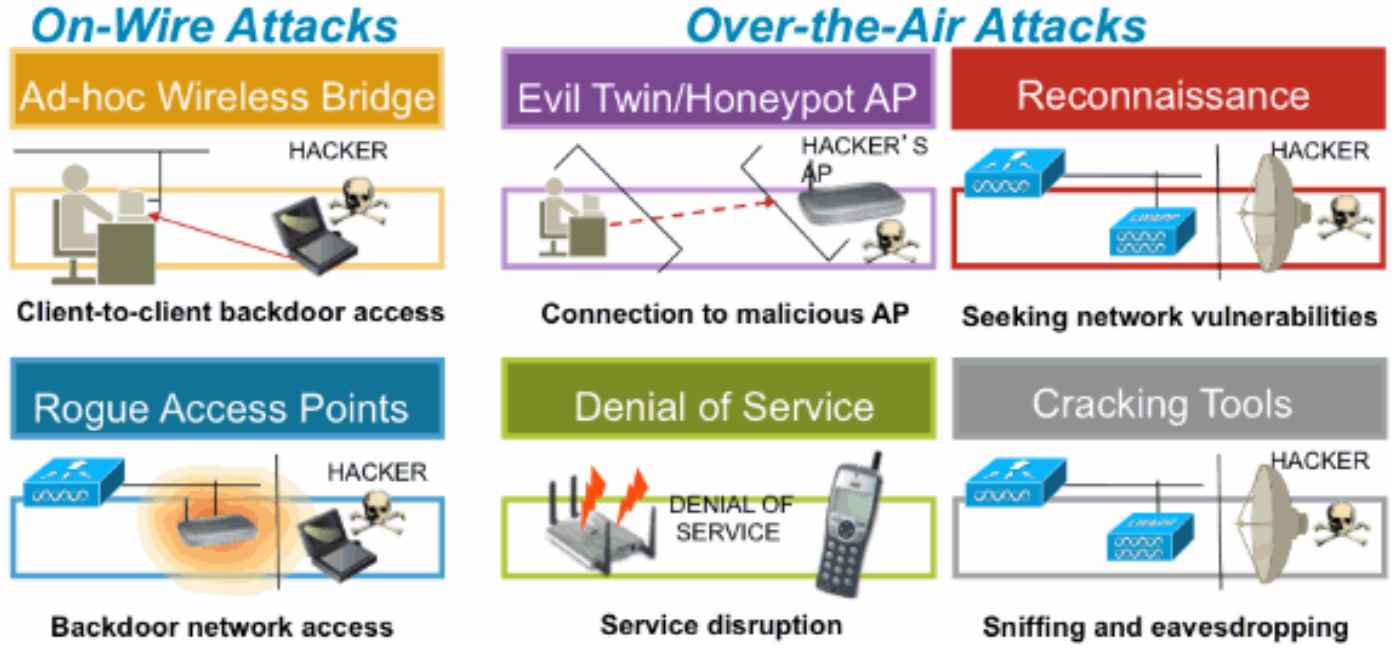


图2 -顶部无线安全威胁



先决条件

要求

本文档没有任何特定的要求。

使用的组件

榆木必需的组件和最小编码版本

- 无线局域网控制器(WLC) -版本7.0.116.xx或以上
- AP -版本7.0.116.xx或以上
- 无线控制系统(WCS) -版本7.0.172.xx或以上
- 移动服务引擎-版本7.0.201.xx或以上

支持的WLC平台

WLC5508、WLC4400、WLC 2106,WLC2504， WiSM-1和WiSM-2WLC平台支持榆木。

支持的AP

11n AP支持榆木包括3500， 1250， 1260， 1040和1140。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

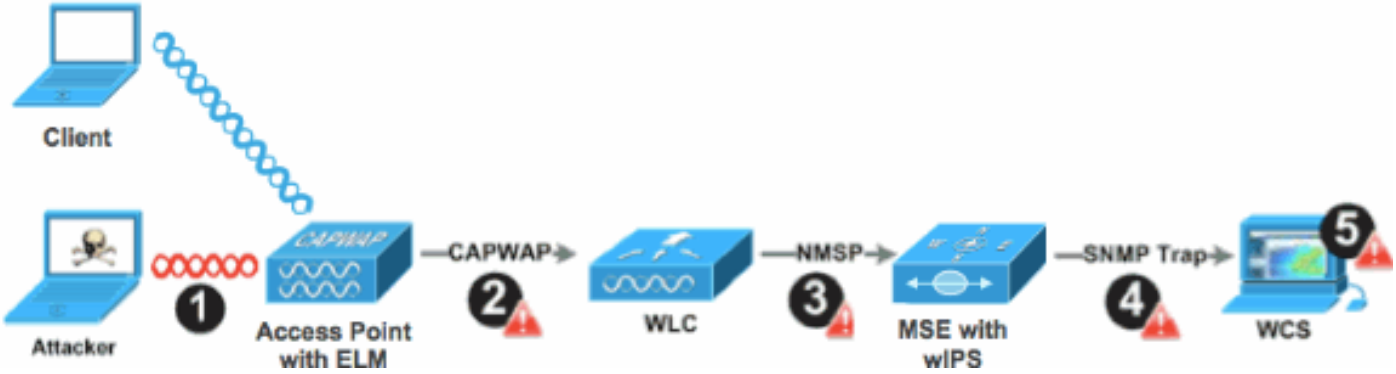
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

榆木wIPS报警流

当他们在委托基础设施AP时，发生攻击只是相关的。榆木AP将检测并且通信到控制器并且关联与报告的MSE与WCS管理。图3提供报警流从管理员的观点：

1. 攻击启动基础设备(“委托的” AP)
2. 检测在通过CAPWAP被传达的榆木AP对WLC
3. 通过透明地对MSE通过NMSP
4. 在MSE的登录的wIPS数据库发送对WCS通过SNMP陷阱
5. 显示在WCS

图3 -威胁检测和报警流



榆木的部署注意事项

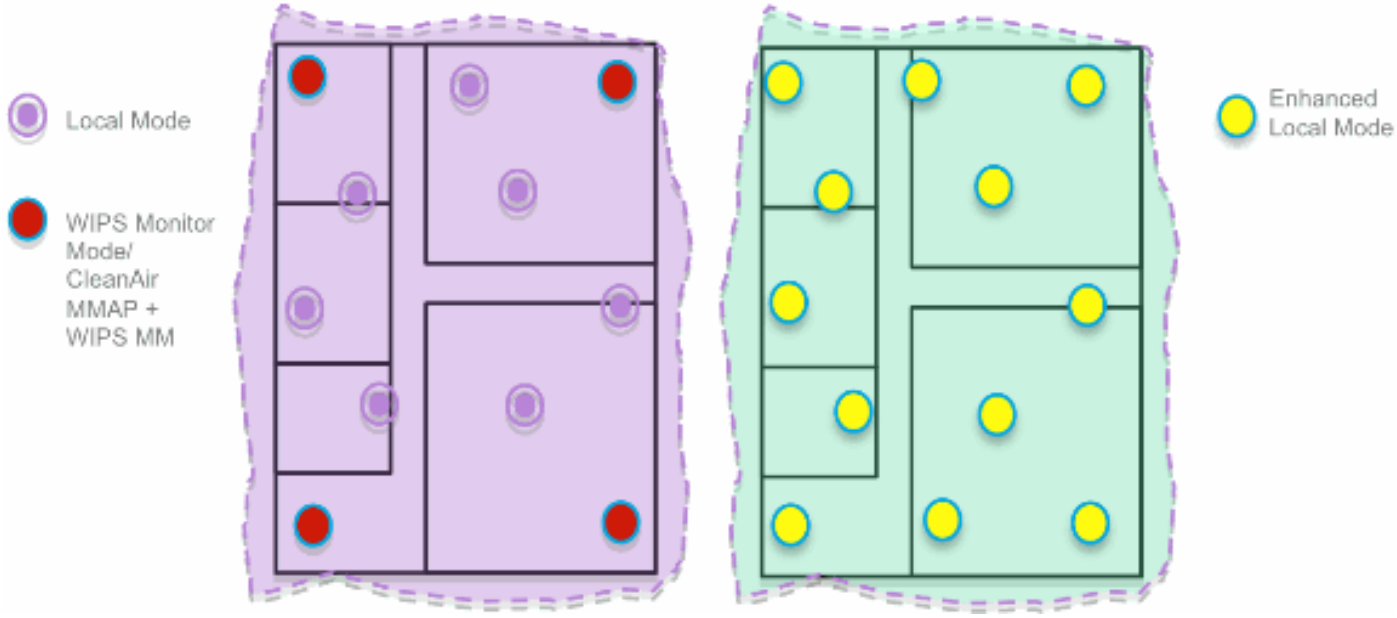
思科建议通过启用在每个AP的榆木在网络满足多数客户安全需要，当网络重叠和开销是考虑事项的一部分。榆木主要的功能为在信道攻击有效运行，不用任何妥协对性能在数据、语音和视频客户端和服务。

榆木与专用的MM

图4提供在wIPS MM之间AP和榆木的标准的部署的一一般对比度。在复核，两种模式的典型的覆盖范围建议：

- 专用的wIPS MM AP典型地包括15,000-35,000平方英尺
- 客户端服务AP从3,000-5,000平方英尺将典型地覆盖

图4 - MM重叠与所有榆木AP



在传统可适应wIPS部署，思科推荐1个MM AP比与每5本地传送方式AP，可能也变化基于最好的覆盖的网络设计和专家指导。通过考虑榆木，管理员启用所有的榆木软件功能现有AP，有效添加MM wIPS操作到本地数据服务模式AP，当维护性能时。

在信道和脱离信道性能

MM AP使用100%无线电？扫描所有信道的s时间，因为它不服务任何WLAN客户端。榆木的主要的功能为在信道攻击有效运行，不用任何妥协对性能在数据、语音和视频客户端和服务。主要的区别在本地传送方式变化的脱离信道扫描;根据活动，脱离信道扫描提供最小停留时间采集足够的有用的资料分类和确定攻击。示例可能是关联，并且其中AP的语音客户端？s RRM扫描延迟，直到语音客户端被分离确保服务不受影响。对于此考虑事项，在脱离信道期间的榆木检测被认为最佳效果。操作在所有的相邻的榆木AP，国家或者DCA信道增加效果，因此建议启用的榆木在每个本地传送方式AP最大保护覆盖的。如果需求全时是为在所有信道的专用的扫描，建议将是部署MM AP。

这些点查看本地传送方式和MM AP差异：

- 本地传送方式AP -有时间分割脱离信道扫描的服务WLAN客户端，细听在每个信道和功能可配置扫描的50ms所有/country/DCA信道的。
- 监控模式AP -不服务WLAN客户端，投入只扫描，细听在每个信道的1.2s，并且扫描所有信道。

在广域网链路间的榆木

思科做巨大努力为了优化在富挑战性方案的功能，例如部署在低带宽广域网链路间的榆木AP。榆木功能在确定介入预先处理攻击签名在AP和优化在低速链接工作。作为最佳实践，推荐测试和测量基准验证与榆木的性能在广域网。

CleanAir集成

榆木功能高度恭维与相似的性能的CleanAir操作和好处对MM AP的部署与这些现有CleanAir光谱意识好处：

- 专用的硅级别RF智能
- 光谱意识，自恢复性能和赛弗优化
- 非标准信道威胁和干扰侦察和缓解
- 非wi-fi检测例如蓝牙、微波、无绳电话等等。
- 检测并且找出RF层DOS攻击例如RF干扰发射台

榆木功能与优点

- 在数据服务本地和H-REAP AP的可适应wIPS扫描
- 没有要求一个分开的覆盖网络的保护
- 联机作为现有wIPS客户的自由SW下载
- 支持无线LAN的PCI标准
- 全双工802.11和non-802.11攻击检测
- 添加辩论术和报告功能
- 集成存在CUWM和WLAN管理
- 灵活性设置集成或专用的MM AP
- 在AP的预处理最小化数据回程(即在非常低带宽链路工作)
- 在服务数据的低影响

许可授权的榆木

榆木wIPS添加一个新的许可证到排序：

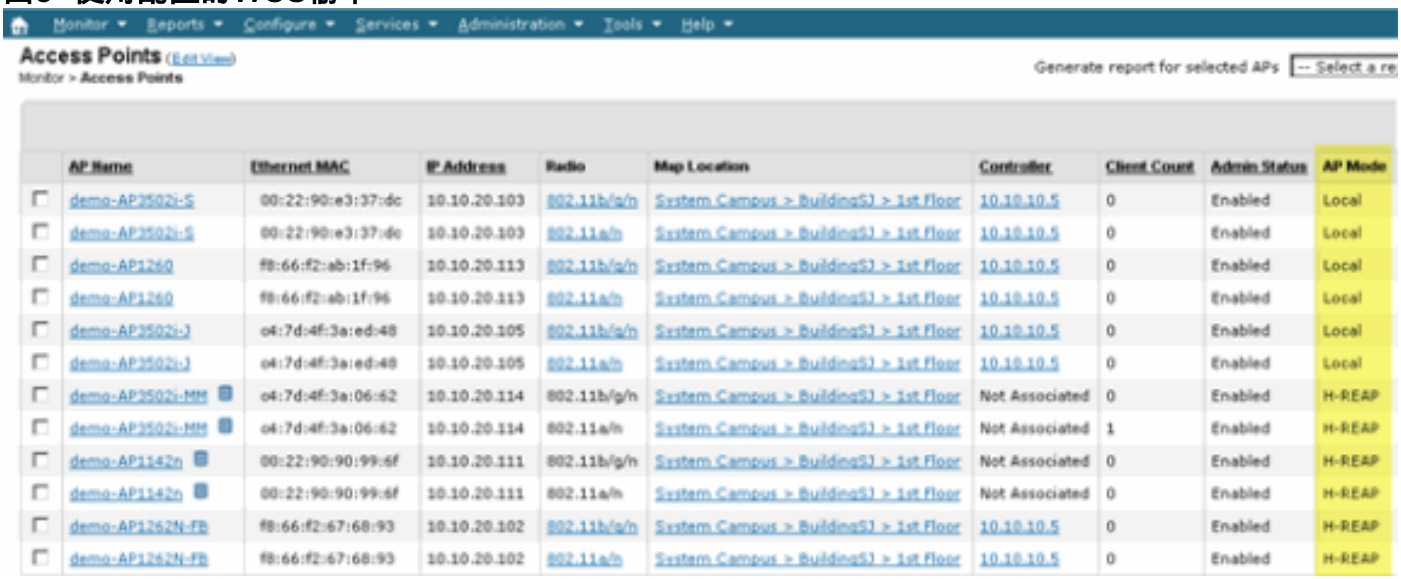
- AIR LMWIPS XX -思科榆木wIPS许可证
- AIR WIPS APxx - Cisco无线wIPS许可证

另外的榆木许可授权的笔记：

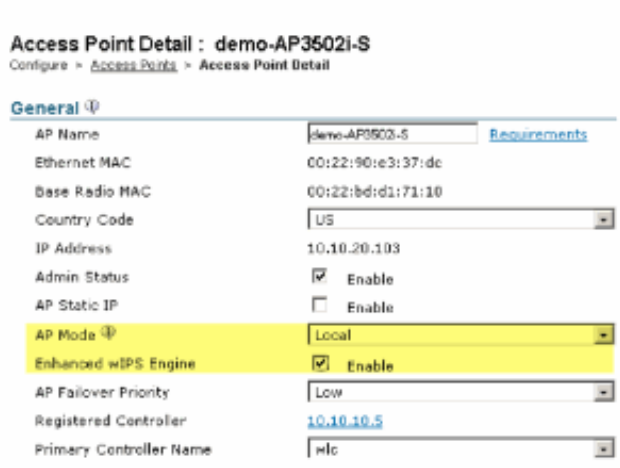
- 如果wIPS MM AP许可证SKU已经安装，那些许可证可能也用于榆木AP。
- wIPS许可证和榆木许可证一起计数往wIPS引擎的平台许可证限额;在3310的2000 AP和3000 AP在335x，分别。
- 评估许可证将包括10 AP wIPS的和10榆木的期限60天。在榆木之前，评估许可证允许20个wIPS MM AP。必须符合支持榆木的软件版本最低要求。

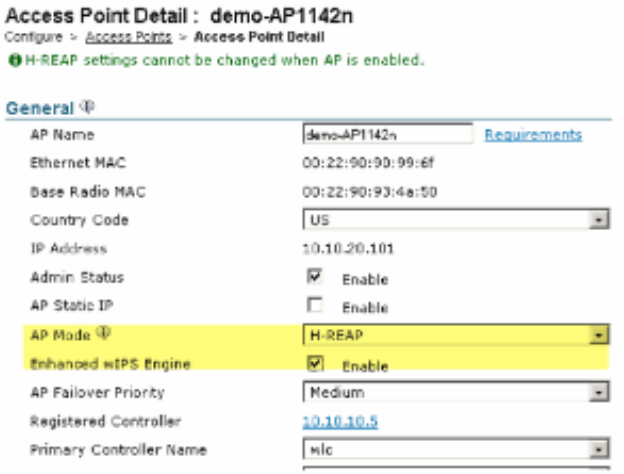
配置与WCS的榆木

图5 -使用配置的WCS榆木

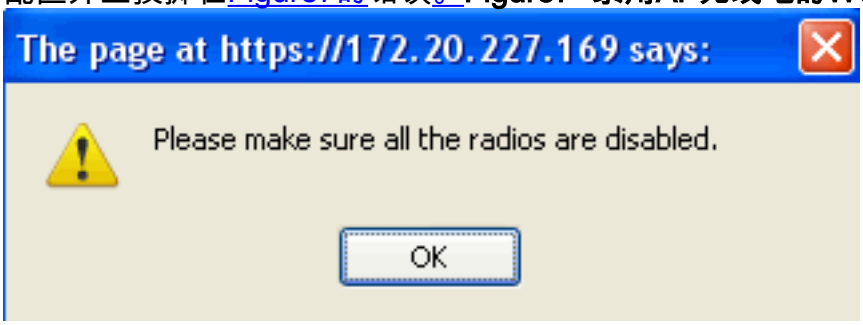


1. 从WCS，在启用前禁用802.11b/g和802.11a AP的无线电？增强版wIPS引擎。？**注意：** 所有相关的客户端将被断开和不会加入，直到无线电启用。
2. 配置一个AP或者请使用WCS配置模板多个轻量AP。[请参阅图 6。](#) **图6 -启动增强版wIPS引擎(榆木) sub模式**

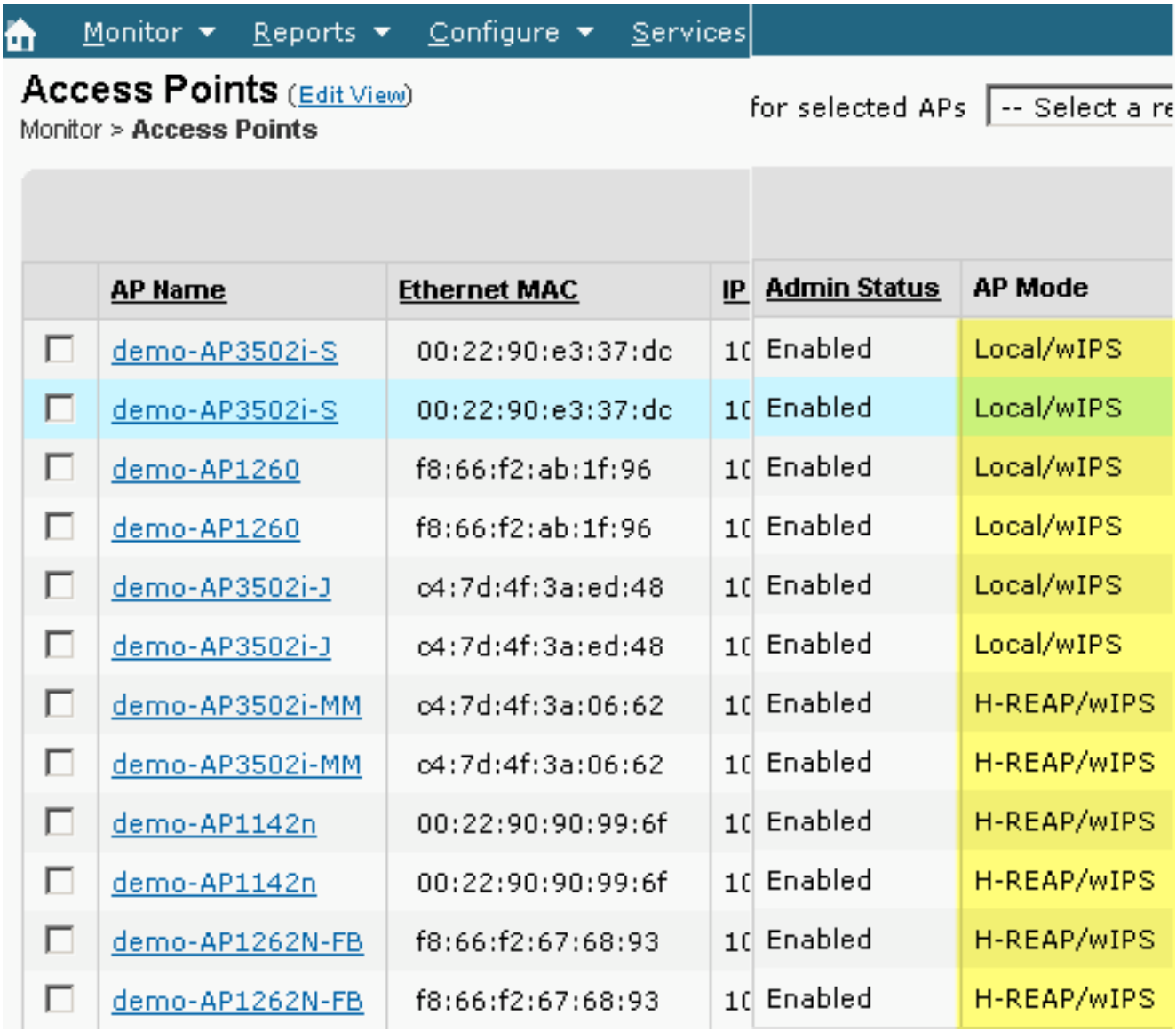




3. 选择**增强版wIPS引擎**，并且点击**"Save"**。启用增强版wIPS引擎不会造成AP重新启动。支持H-REAP;启用方式和一样本地传送方式AP的。**注意：** 如果此AP无线电之一启用， WCS将忽略配置并且投掷在[Figure7的](#)错误。**Figure7 -禁用AP无线电的WCS提醒在启用榆木前**



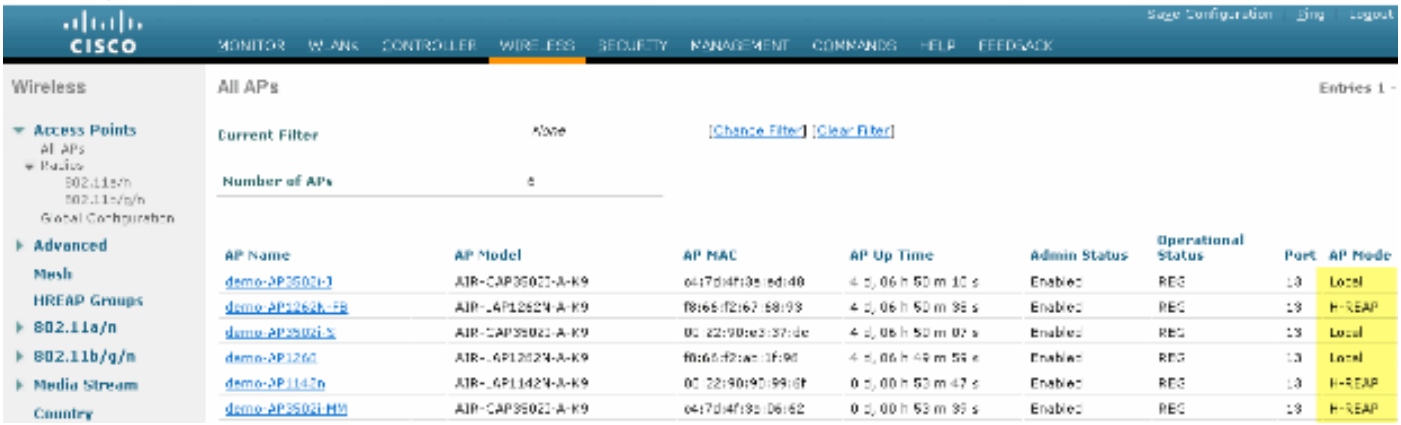
4. 配置成功可以通过观察在AP模式上的变化验证从？本地或H-REAP ？对**本地/wIPS或H-REAP/wIPS。**[请参阅图 8。](#) **图8 -显示AP模式的WCS包括与本地和H-REAP的wIPS**



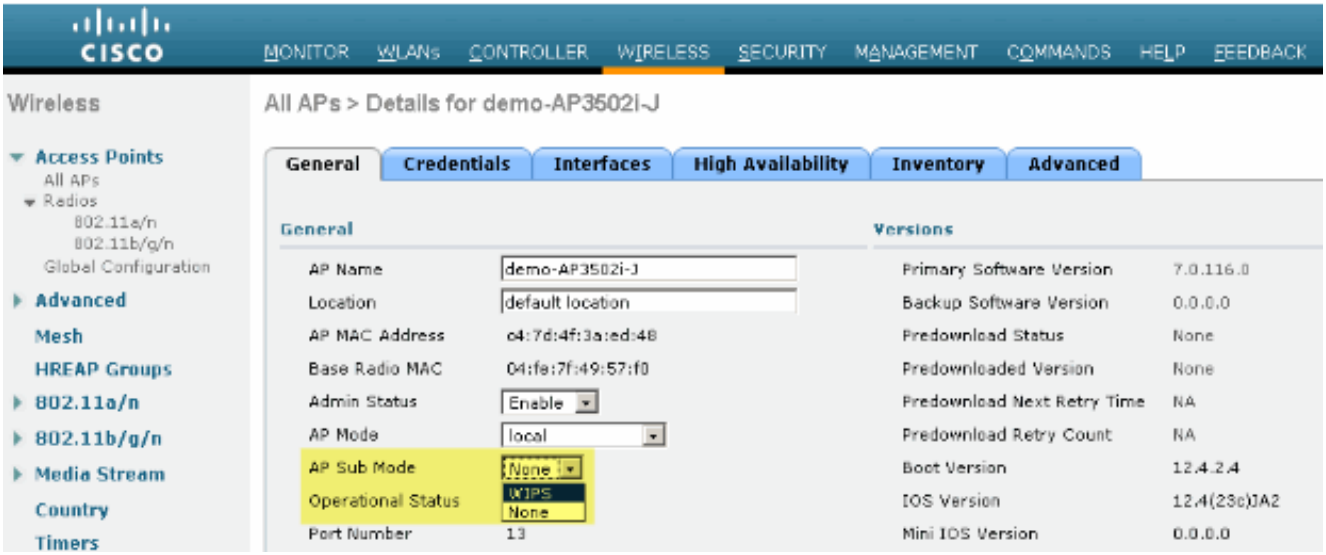
5. 启用哪里禁用在Step1的无线电。
6. 创建wIPS配置文件并且推送它到控制器为了配置能完成。**注意**： 关于wIPS的完整的配置信息，参考思科可适应wIPS部署指南。

从WLC的配置

图9 -配置与WLC的榆木



1. 从**Wireless选项卡**选择AP。**图10 -更改AP子模式的WLC包括wIPS榆木**



2. 从AP Sub模式下拉菜单，请选择**wIPS** (图10)。
3. 运用，然后保存配置。

注意： 为了使工作榆木的功能， MSE和WCS要求与许可授权的wIPS。更改从单独WLC的AP sub模式不会启用榆木。

在榆木检测的攻击

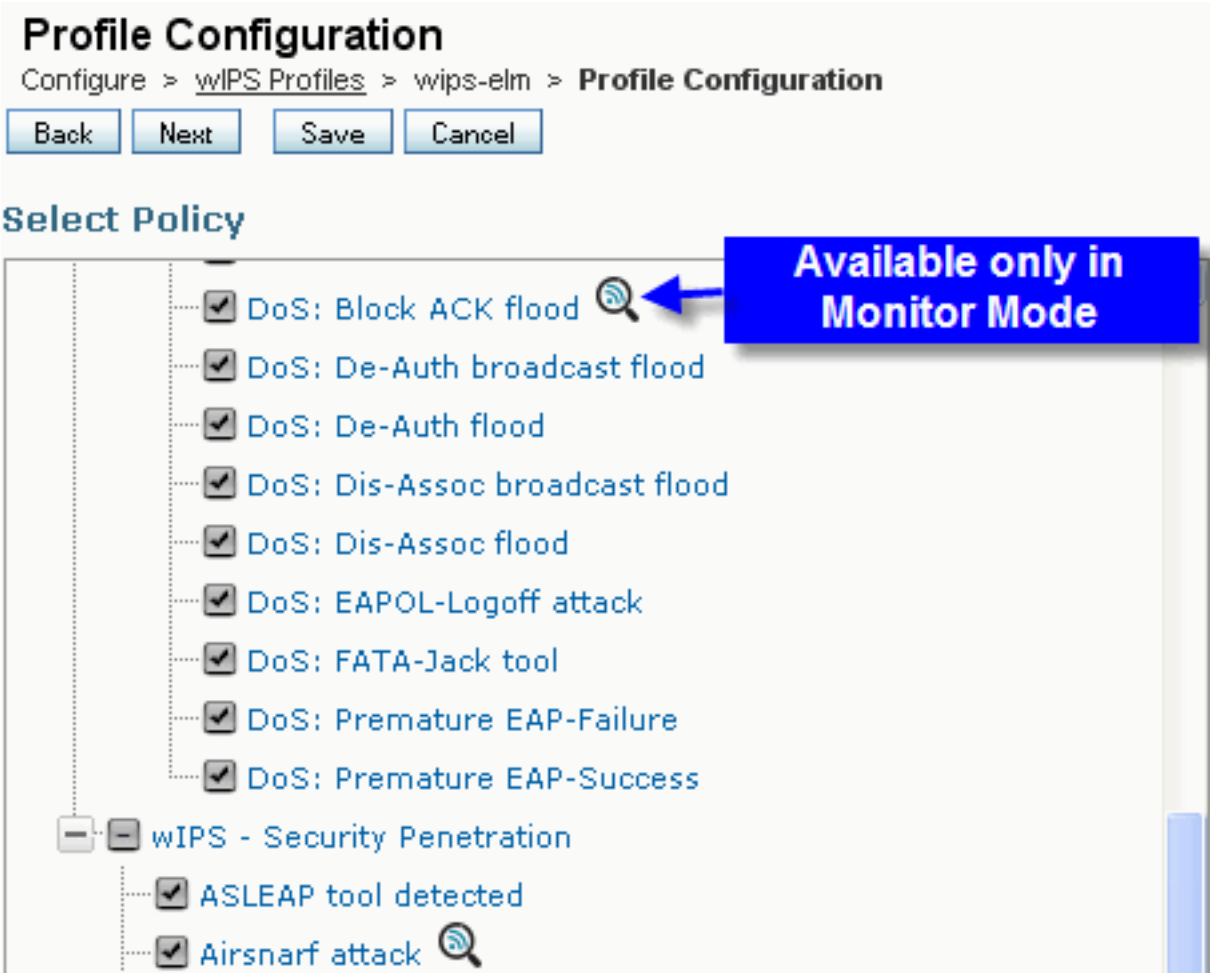
表1 - wIPS签名支持矩阵

检测的攻击	榆木	MM
AP的DOS攻击		
关联充斥	Y	Y
关联表溢出	Y	Y
验证充斥	Y	Y
EAPOL开始攻击	Y	Y
PS-Poll充斥	Y	Y
探测器请求充斥	N	Y
未经鉴定的关联	Y	Y
基础设施的DOS攻击		
CTS充斥	N	Y
昆士兰科技大学检测安全漏洞代码	N	Y
RF阻塞	Y	Y
RTS充斥	N	Y
虚拟载波攻击	N	Y
站点的DOS攻击		
认证失败攻击	Y	Y
块ACK充斥	N	Y
DE验证广播充斥	Y	Y
DE验证充斥	Y	Y
DisAssoc广播充斥	Y	Y
DisAssoc充斥	Y	Y
EAPOL注销攻击	Y	Y

FATA杰克工具	Y	Y
过早的EAP失败	Y	Y
过早的EAP成功	Y	Y
安全渗透攻击		
检测的ASLEAP工具	Y	Y
Airsnarf攻击	N	Y
ChopChop攻击	Y	Y
由WLAN安全异常情况的天零攻击	N	Y
由设备安全性异常情况的天零攻击	N	Y
探查为AP的设备	Y	Y
在EAP方法的词典攻击	Y	Y
802.1x验证的EAP攻击	Y	Y
AP检测的伪造品	Y	Y
检测的假DHCP服务器	N	Y
检测的快速WEP破解工具	Y	Y
碎片攻击	Y	Y
检测的蜂蜜AP	Y	Y
检测的Hotspotter工具	N	Y
不正确的广播帧	N	Y
检测的畸形的802.11数据包	Y	Y
中间攻击的人	Y	Y
Netstumbler检测	Y	Y
检测的Netstumbler受害者	Y	Y
检测的PSPF侵害	Y	Y
软奇AP或检测的主机AP	Y	Y
检测的用欺骗性MAC地址	Y	Y
可疑在检测的几小时流量以后	Y	Y
由供应商列表的未授权的关联	N	Y
未授权的关联检测	Y	Y
Wellenreiter检测	Y	Y

注意： 添加CleanAir也将启动non-802.11攻击的检测。

图11 - WCS wIPS配置文件视图



在表11，请配置从WCS的wIPS配置文件， 图标表明攻击将检测，只有当AP在MM时，当仅最佳效果，当在榆木。

排除故障榆木

检查这些项目：

- 确保NTP配置。
- 确保MSE时间设定在UTC。
- 如果设备组不工作，请使用覆盖配置文件SSID与其中任一。重新启动AP。
- make sure许可授权配置(榆木AP当前使用KAM许可证)
- 如果wIPS配置文件太经常更改，再请同步MSE控制器。确保配置文件是活跃的在WLC。
- 使用MSE CLIs，确保WLC是MSE的一部分：SSH或telnet对您的MSE。执行 **/opt/mse/wips/bin/wips_cli** -此控制台可以用于访问到以下命令到关于可适应wIPS系统的状态的收集信息。**显示wlc全部**？发出在wIPS控制台里面。此命令用于验证积极地通信与在MSE的wIPS服务的控制器。请参阅图 12。**图12 - MSE CLI正在验证与MSE wIPS服务的WLC激活**

```
wIPS>show wlc allWLC MAC Profile ProfileStatus IPOnx Status Status----------------------------------------------------------------------------00:21:55:06:F2:80
WCS-Default Policyactive on controller 172.20.226.197Active
```

- 确保报警获得检测在MSE使用MSE CLIs。**显示报警列表**-发出在wIPS控制台里面。此命令用于列出在wIPS服务数据库内当前包含的报警。密钥字段是唯一哈希密钥分配到特定报警。Type字段是报警种类。此图表在表13显示报警ID和说明列表：**图13 - MSE CLI显示list命令的报警**

```
wIPS>show alarm listKey Type Src MACLastTime Active First Time----------------------------------------------------------89 89 00:00:00:00:00:00
2008/09/0418:19:26 2008/09/07 02:16:58 165631 95 00:00:00:00:00:00 2008/09/0417:18:31
```

```
2008/09/04 17:18:31 01989183 99 00:1A:1E:80:5C:40 2008/09/0418:19:44 2008/09/04 18:19:44 0
```

第一次和上次字段表示时间戳，当报警检测时;这些在UTC时间存储。如果报警当前检测，有效域突出显示。

- 清除MSE数据库。如果遇到MSE数据库损坏，或者没有的情况其他故障排除方法将工作，清除数据库和开始可能是最佳的。**图14 - MSE服务命令**`1. /etc/init.d/msed stop2. Remove the database using the command 'rm/opt/mse/locserver/db/linux/server-eng.db'3. /etc/init.d/msed start`

相关信息

- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- 思科无线控制系统配置指南，版本7.0.172.0
- 技术支持和文档 - Cisco Systems