自适应wIPS ELM配置和部署指南

目录

简介

思科自适应无线入侵防御系统(wIPS)解决方案添加了增强型本地模式(ELM)功能，允许管理员使用其已部署的接入点(AP)提供全面保护，而无需单独的重叠网络(图1)。在ELM之前和传统自适应wIPS部署中，需要专用监控模式(MM)AP来提供PCI合规性需求或保护，防止未经授权的安全访问、渗透和攻击(图2)。ELM可有效提供同类产品，简化无线安全实施，同时降低资本支出和运营成本。本文档仅重点介绍ELM，不会修改任何现有wIPS部署优势与MM AP。

图1 — 增强型本地模式AP部署

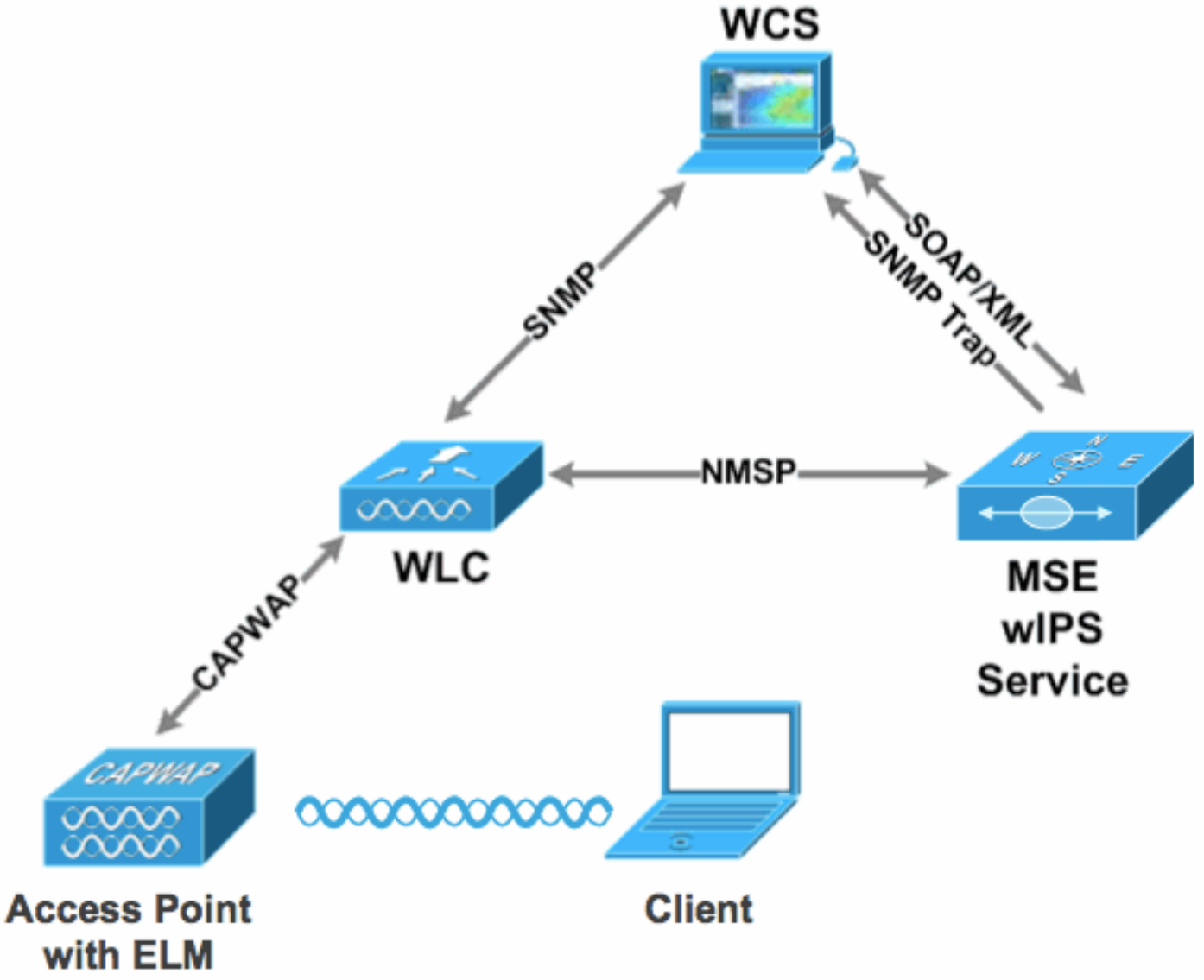
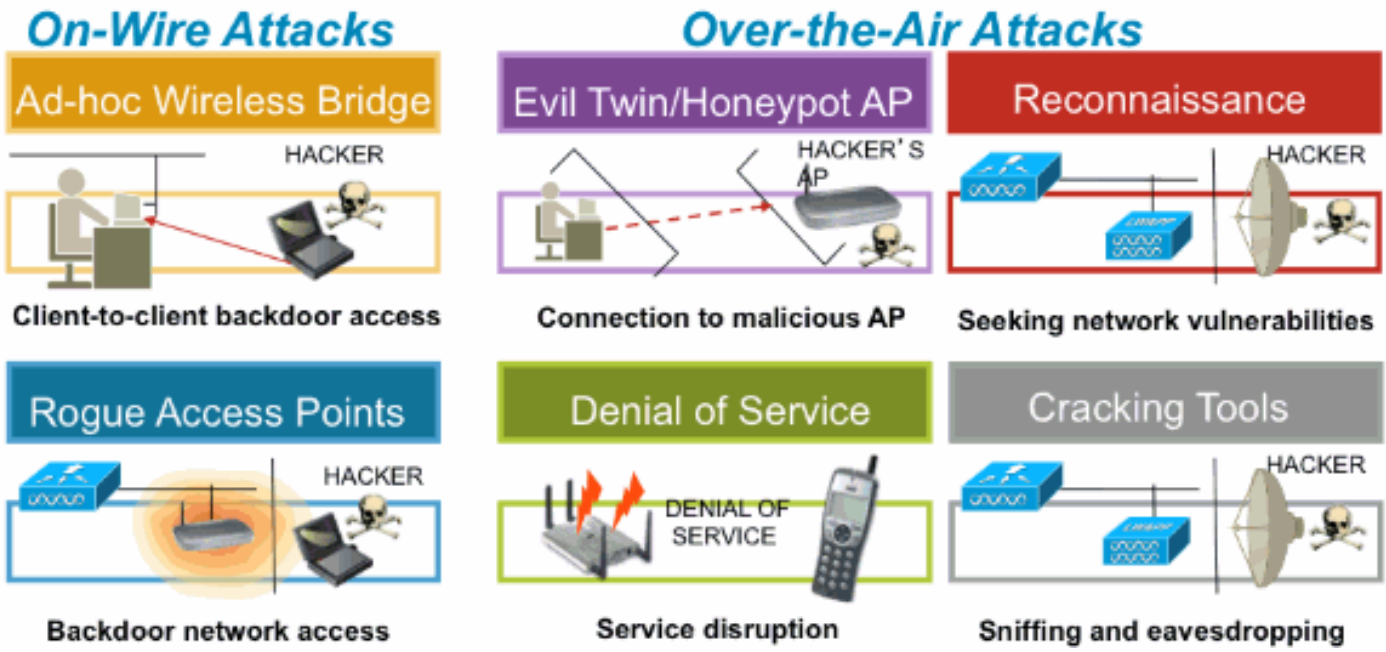

WCS
SNMP
SOAP/XML
SNMP Trap
NMSP
WLC
MSE
wIPS
Service
CAPWAP
CAPWAP
Access Point
with ELM
Client

图2 — 主要无线安全威胁


On-Wire Attacks
Over-the-Air Attacks
Ad-hoc Wireless Bridge
HACKER
Client-to-client backdoor access
Evil Twin/Honeypot AP
HACKER'S AP
Connection to malicious AP
Reconnaissance
HACKER
Seeking network vulnerabilities
Rogue Access Points
HACKER
Backdoor network access
Denial of Service
DENIAL OF SERVICE
Service disruption
Cracking Tools
HACKER
Sniffing and eavesdropping

先决条件

要求

本文档没有任何特定的要求。

使用的组件

ELM必需组件和最低代码版本

- 无线LAN控制器(WLC)- 7.0.116.xx或更高版本
- AP — 版本7.0.116.xx或更高版本
- 无线控制系统(WCS)- 7.0.172.xx或更高版本
- 移动服务引擎 — 7.0.201.xx或更高版本

支持WLC平台

WLC5508、WLC4400、WLC 2106、WLC2504、WiSM-1和WiSM-2WLC平台上支持ELM。

支持AP

11n AP（包括3500、1250、1260、1040和1140）支持ELM。

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

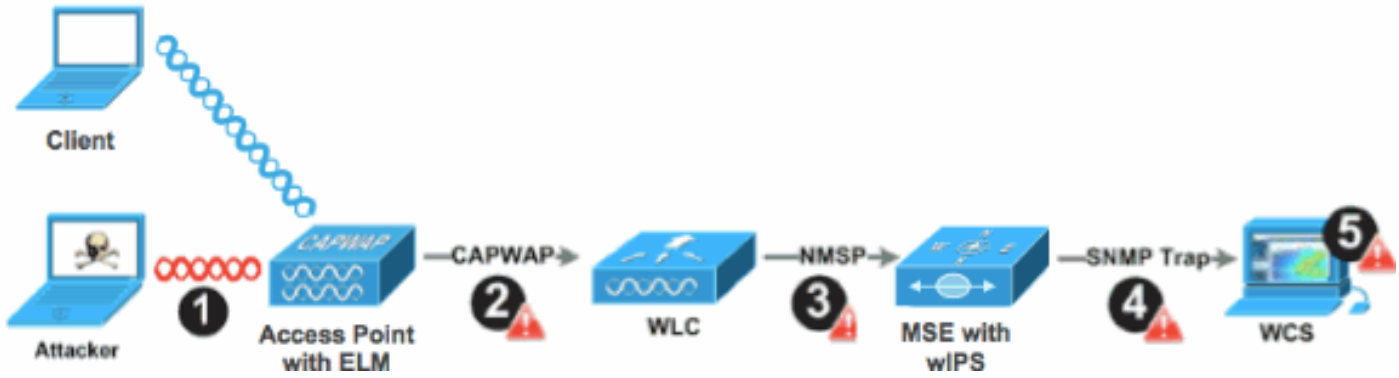
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

ELM wIPS警报流

仅当攻击发生在受信任的基础设施AP上时，它们才相关。ELM AP将检测控制器并与控制器通信，并与MSE关联以便通过WCS管理进行报告。图3从管理员的角度提供了警报流程：

1. 对基础设施设备（“可信”AP）发起的攻击
2. 在通过CAPWAP与WLC通信的ELM AP上检测到
3. 通过NMSP透明传递给MSE
4. 登录MSE上的wIPS数据库通过SNMP陷阱发送到WCS
5. 在WCS中显示

图3 — 威胁检测和警报流程



ELM的部署注意事项

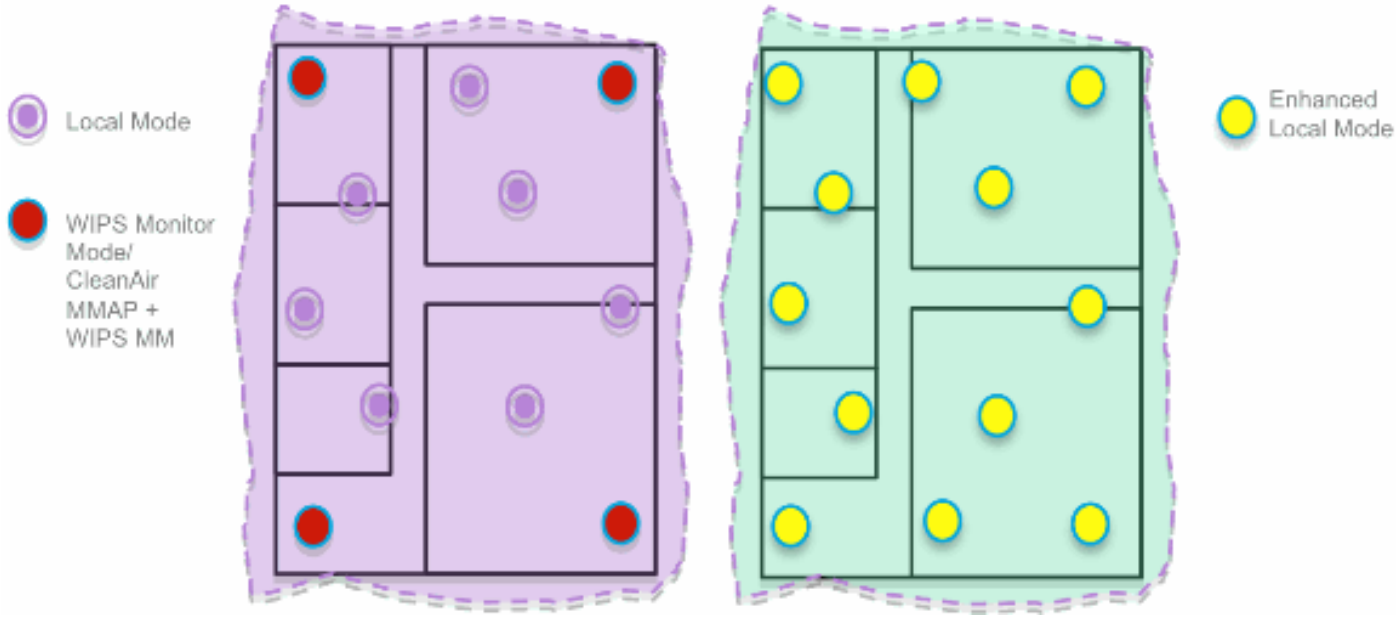
思科建议，当考虑网络重叠和/或成本时，通过在网络上的每个AP上启用ELM来满足大多数客户的安全需求。ELM主要功能可有效应对信道内攻击，而不会影响数据、语音和视频客户端以及服务的性能。

ELM与专用MM

图4提供了wIPS MM AP和ELM的标准部署之间的常规对比图。在回顾中，两种模式的典型覆盖范围均表明：

- 专用wIPS MM AP通常覆盖15,000-35,000平方英尺
- 客户端服务AP通常覆盖3,000-5,000平方英尺

图4 - MM与所有ELM AP的重叠



在传统自适应wIPS部署中，思科建议每5个本地模式AP配置1 MM AP，此比例可能因网络设计和专家指导而异，以实现最佳覆盖范围。通过考虑ELM，管理员只需为所有现有AP启用ELM软件功能，从而在保持性能的同时，将MM wIPS操作有效地添加到本地数据服务模式AP。

信道内和信道外性能

MM AP使用无线电的100%时间扫描所有信道，因为它不为任何WLAN客户端提供服务。ELM的主要功能可有效应对信道内攻击，而不会影响数据、语音和视频客户端及服务的性能。主要区别在于本地模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，以收集足够的可用于分类和确定攻击的信息。示例可能涉及关联的语音客户端，其中AP的RRM扫描会延迟到取消关联语音客户端，以确保服务不受影响。因此，信道外期间ELM检测被视为尽力而为。运行于所有、国家/地区或DCA信道的相邻ELM AP可提高效率，因此建议在每个本地模式AP上启用ELM，以实现最大保护覆盖范围。如果要求在所有信道上进行全时专用扫描，则建议部署MM AP。

以下要点回顾本地模式和MM AP的差异：

- 本地模式AP — 为WLAN客户端提供时间分割的脱离信道扫描，在每个信道上侦听50毫秒，并为所有/国家/地区/DCA信道提供可配置扫描。
- 监控模式AP — 不为WLAN客户端提供服务（仅用于扫描），侦听每个信道上的1.2秒，并扫描所有信道。

跨WAN链路的ELM

思科已做出巨大努力来优化各种挑战性场景中的功能，例如跨低带宽WAN链路部署ELM AP。ELM功能涉及在AP确定攻击特征码时的预处理，并经过优化以适用于慢速链路。作为最佳实践，建议测试和测量基准，以验证WAN上ELM的性能。

CleanAir集成

ELM功能高度完善CleanAir操作，其性能和优势与MM AP部署相似，并具有以下现有CleanAir频谱感知优势：

- 专用硅级RF智能
- 频谱感知、自我修复和自我优化
- 非标准信道威胁和干扰检测和缓解
- 非Wi-Fi检测，例如蓝牙、微波炉、无绳电话等。
- 检测并定位RF层DOS攻击，例如RF干扰器

ELM功能和优势

- 为本地和H-REAP AP提供服务的数据中的自适应wIPS扫描
- 无需单独的重叠网络即可提供保护
- 可供现有wIPS客户免费下载

- 支持无线局域网的PCI合规性
- 完整的802.11和非802.11攻击检测
- 增加调查分析和报告功能
- 与现有CUWM和WLAN管理集成
- 灵活设置集成或专用MM AP
- AP的预处理，最大程度地减少了数据回传（即工作在带宽非常低的链路上）
- 对服务数据的影响较低

ELM许可

ELM wIPS在订购中添加了一个新许可证：

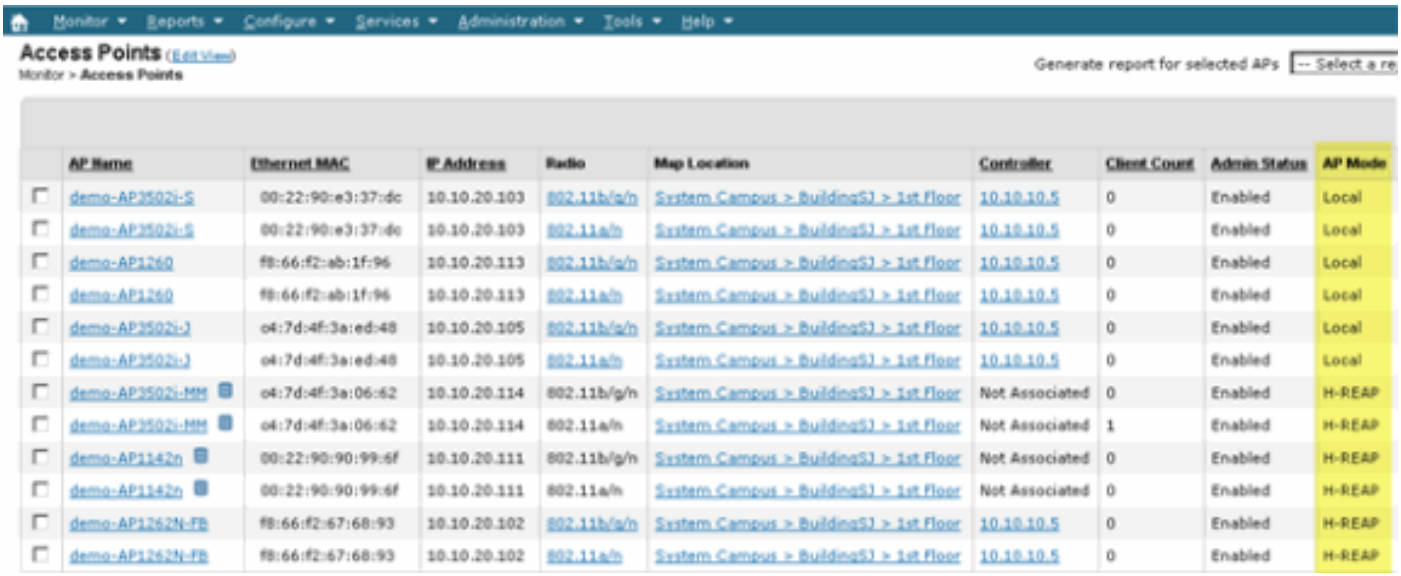
- AIR-LM-WIPS-xx - Cisco ELM wIPS许可证
- AIR-WIPS-AP-xx — 思科无线wIPS许可证

其他ELM许可说明：

- 如果已安装wIPS MM AP许可证SKU，则这些许可证也可以用于ELM AP。
- wIPS许可证和ELM许可证一起计入wIPS引擎的平台许可证限制；3310上分别为2000个AP，335x上分别为3000个AP。
- 评估许可证将包括用于wIPS的10个AP和用于ELM的10个AP，有效期最长为60天。在ELM之前，评估许可证最多允许20个wIPS MM AP。必须满足支持ELM的软件版本的最低要求。

使用WCS配置ELM

图5 — 使用WCS配置ELM

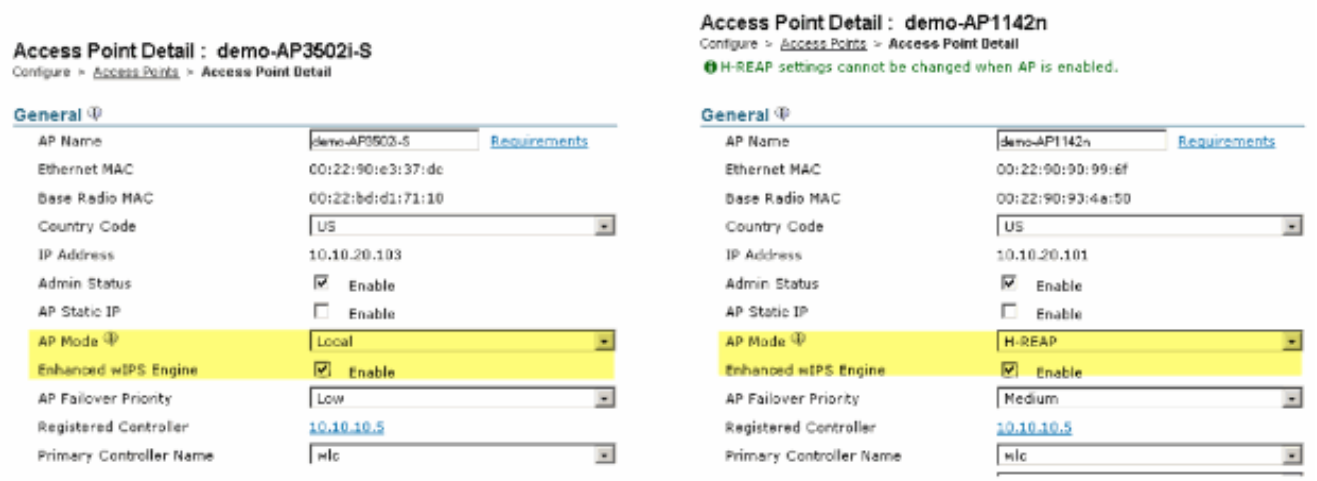


1. 在WCS中，在启用“增强型wIPS引擎”之前禁用AP的802.11b/g和802.11a无线电。

   注意：所有关联的客户端将断开连接，并且在无线电启用之前不会加入。

2. 配置一个AP，或者对多个轻量AP使用WCS配置模板。请参阅图 6。

   图6 — 启用增强型wIPS引擎(ELM)子模式



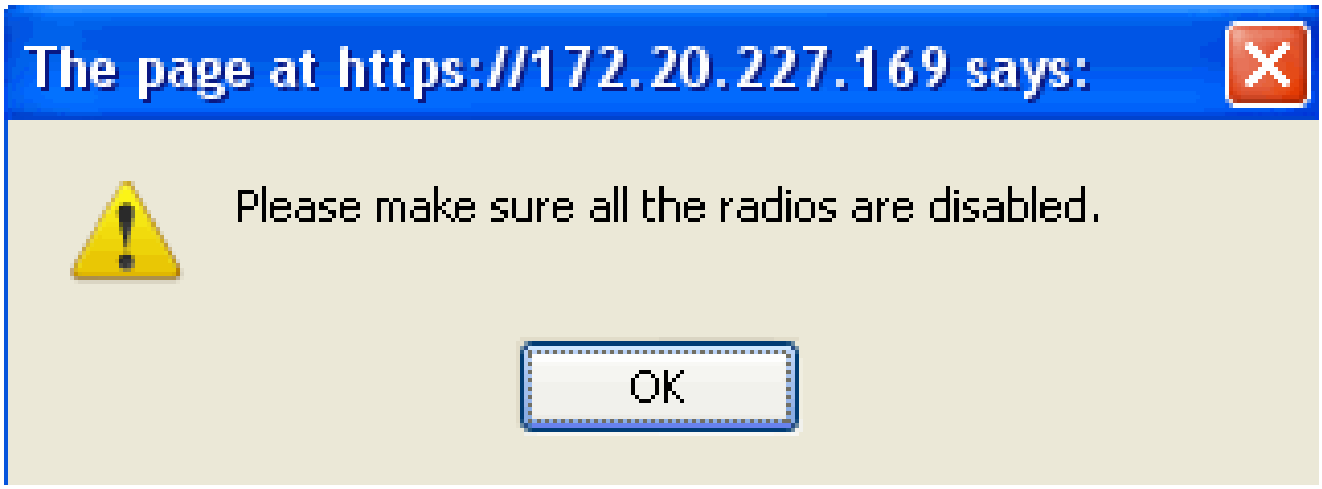
3. 选择Enhanced wIPS Engine，然后单击Save。

   a. 启用增强型wIPS引擎不会导致AP重新启动。

   b. 支持H-REAP；启用方式与本地模式AP相同。

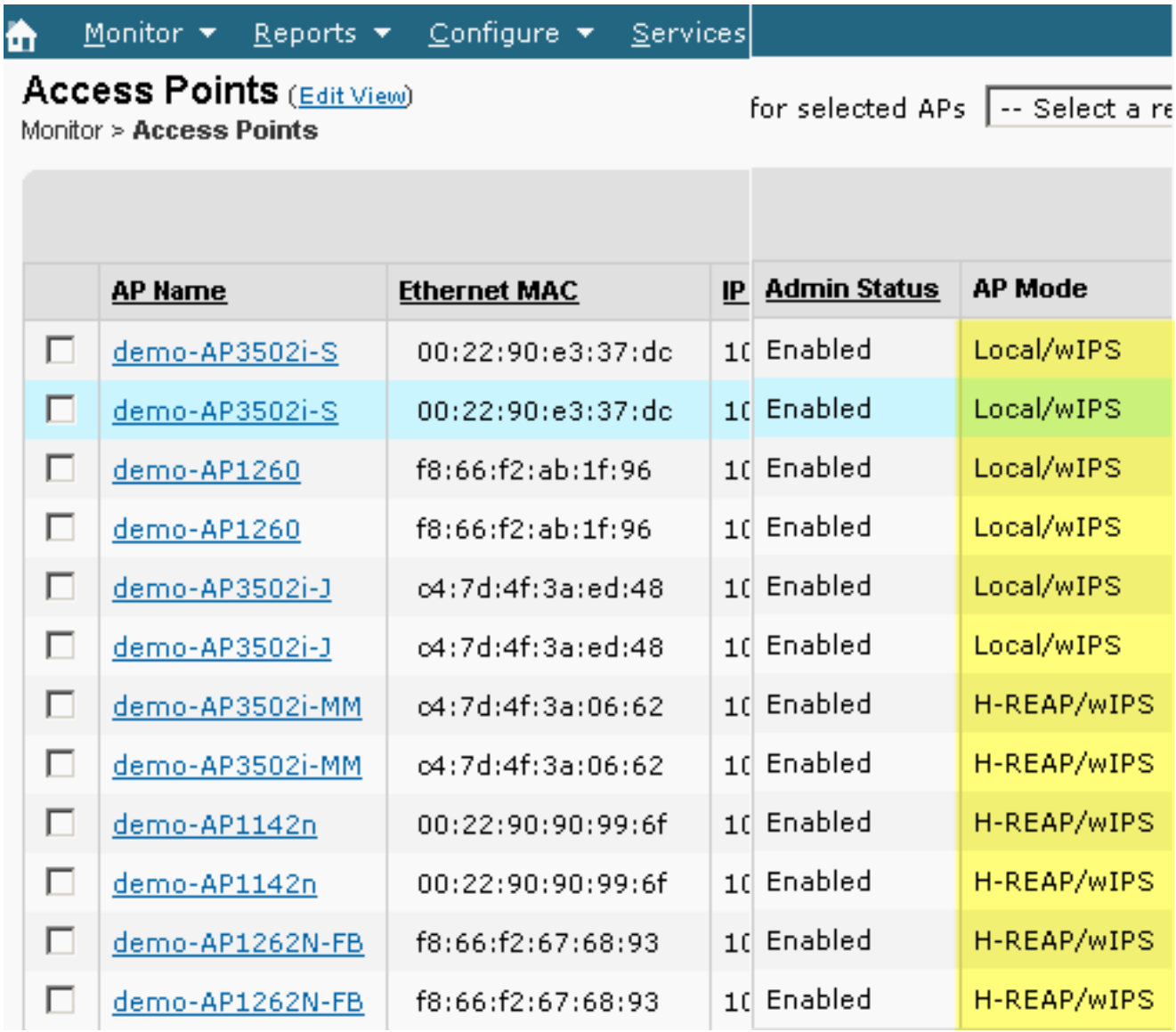
注意：如果启用了此AP的任一无线电，WCS将忽略配置并引发图7中的错误。

图7 — 启用ELM之前禁用AP无线电的WCS提醒



4. 可以通过观察AP模式从“Local or H-REAP”更改为Local/wIPS或H-REAP/wIPS来验证配置是否成功。请参阅图 8。

图8 - WCS显示AP模式以包括wIPS与本地和/或H-REAP



	AP Name	Ethernet MAC	IP	Admin Status	AP Mode
☐	demo-AP3502i-S	00:22:90:e3:37:dc	10	Enabled	Local/wIPS
☐	demo-AP3502i-S	00:22:90:e3:37:dc	10	Enabled	Local/wIPS
☐	demo-AP1260	f8:66:f2:ab:1f:96	10	Enabled	Local/wIPS
☐	demo-AP1260	f8:66:f2:ab:1f:96	10	Enabled	Local/wIPS
☐	demo-AP3502i-J	c4:7d:4f:3a:ed:48	10	Enabled	Local/wIPS
☐	demo-AP3502i-J	c4:7d:4f:3a:ed:48	10	Enabled	Local/wIPS
☐	demo-AP3502i-MM	c4:7d:4f:3a:06:62	10	Enabled	H-REAP/wIPS
☐	demo-AP3502i-MM	c4:7d:4f:3a:06:62	10	Enabled	H-REAP/wIPS
☐	demo-AP1142n	00:22:90:90:99:6f	10	Enabled	H-REAP/wIPS
☐	demo-AP1142n	00:22:90:90:99:6f	10	Enabled	H-REAP/wIPS
☐	demo-AP1262N-FB	f8:66:f2:67:68:93	10	Enabled	H-REAP/wIPS
☐	demo-AP1262N-FB	f8:66:f2:67:68:93	10	Enabled	H-REAP/wIPS

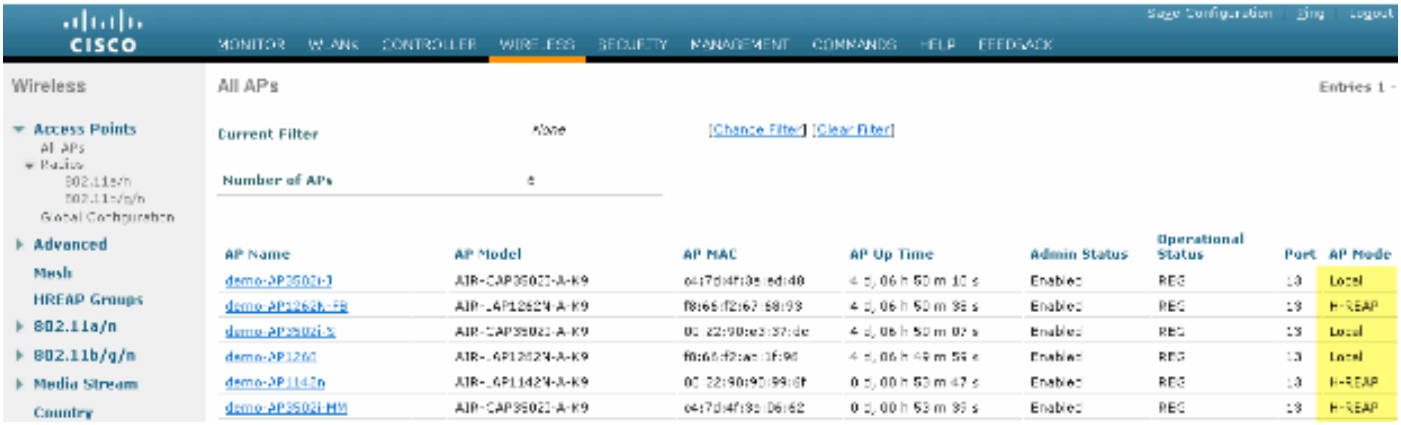
5. 启用第1步中禁用的无线电。

6. 创建wIPS配置文件并将其推送到控制器，以便完成配置。

注意：有关wIPS的完整配置信息，请参阅Cisco自适应wIPS部署指南。

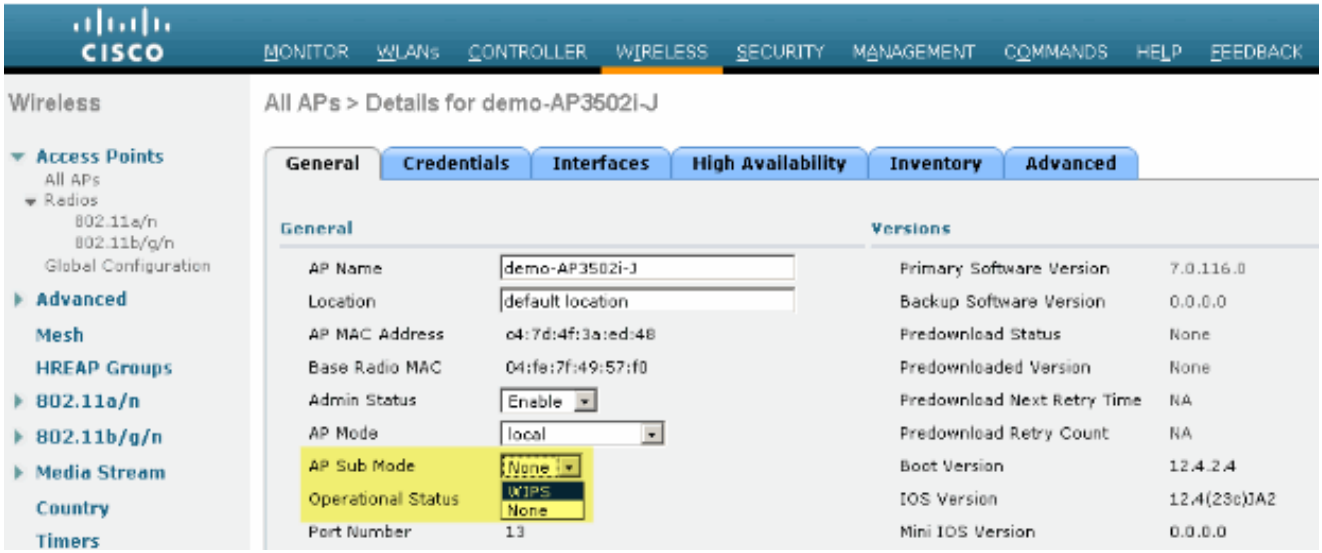
从WLC配置

图9 — 使用WLC配置ELM



1. 从Wireless选项卡中选择AP。

图10 - WLC将AP子模式更改为包括wIPS ELM



2. 从AP子模式下拉菜单中，选择wIPS(图10)。

3. 应用，然后保存配置。

注意：要使ELM功能正常工作，需要wIPS许可支持MSE和WCS。仅从WLC更改AP子模式不会启用ELM。

在ELM中检测到的攻击

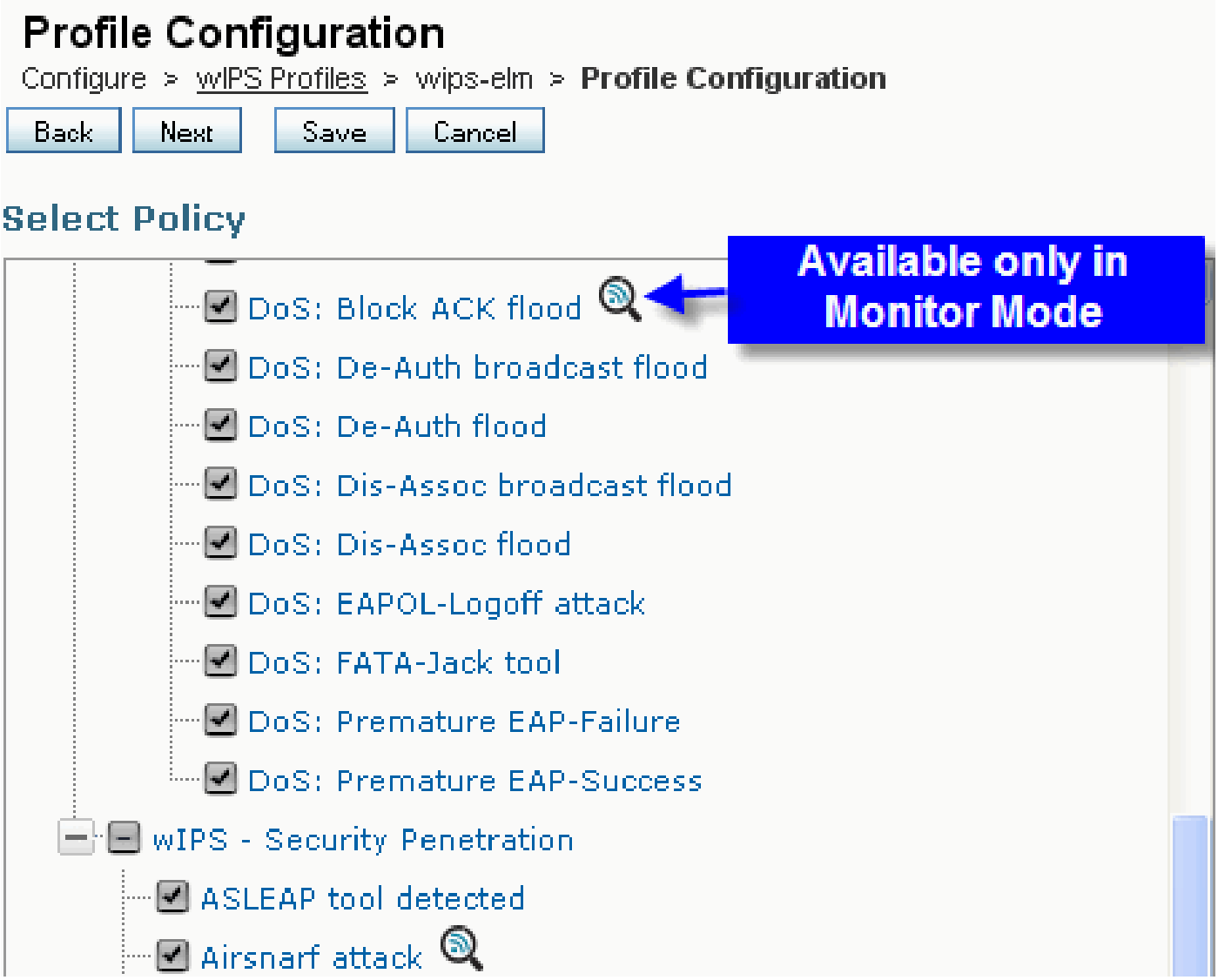
表1 - wIPS签名支持表

检测到的攻击	ELM	MM
针对AP的DoS攻击		
关联泛洪	Y	Y
关联表溢出	Y	Y
身份验证泛洪	Y	Y
EAPOL-Start攻击	Y	Y
PS-Poll泛洪	Y	Y
探测请求泛洪	n	Y
未经身份验证的关联	Y	Y
针对基础设施的DoS攻击		
CTS泛洪	n	Y
昆士兰科技大学开发	n	Y
射频干扰	Y	Y
RTS泛洪	n	Y
虚拟运营商攻击	n	Y
针对站点的DoS攻击		
身份验证失败攻击	Y	Y
阻止ACK泛洪	n	Y
取消身份验证广播泛洪	Y	Y
De-Auth flood	Y	Y
Dis-Assoc广播泛洪	Y	Y
Dis-Assoc泛洪	Y	Y
EAPOL-Logoff攻击	Y	Y
FATA插孔工具	Y	Y
过早的EAP故障	Y	Y
过早的EAP成功	Y	Y
安全渗透攻击		
检测到ASLEAP工具	Y	Y
Airsnarf攻击	n	Y
ChopChop攻击	Y	Y
由WLAN安全异常发起的零日攻击	n	Y
设备安全异常零日攻击	n	Y
AP的设备探测	Y	Y

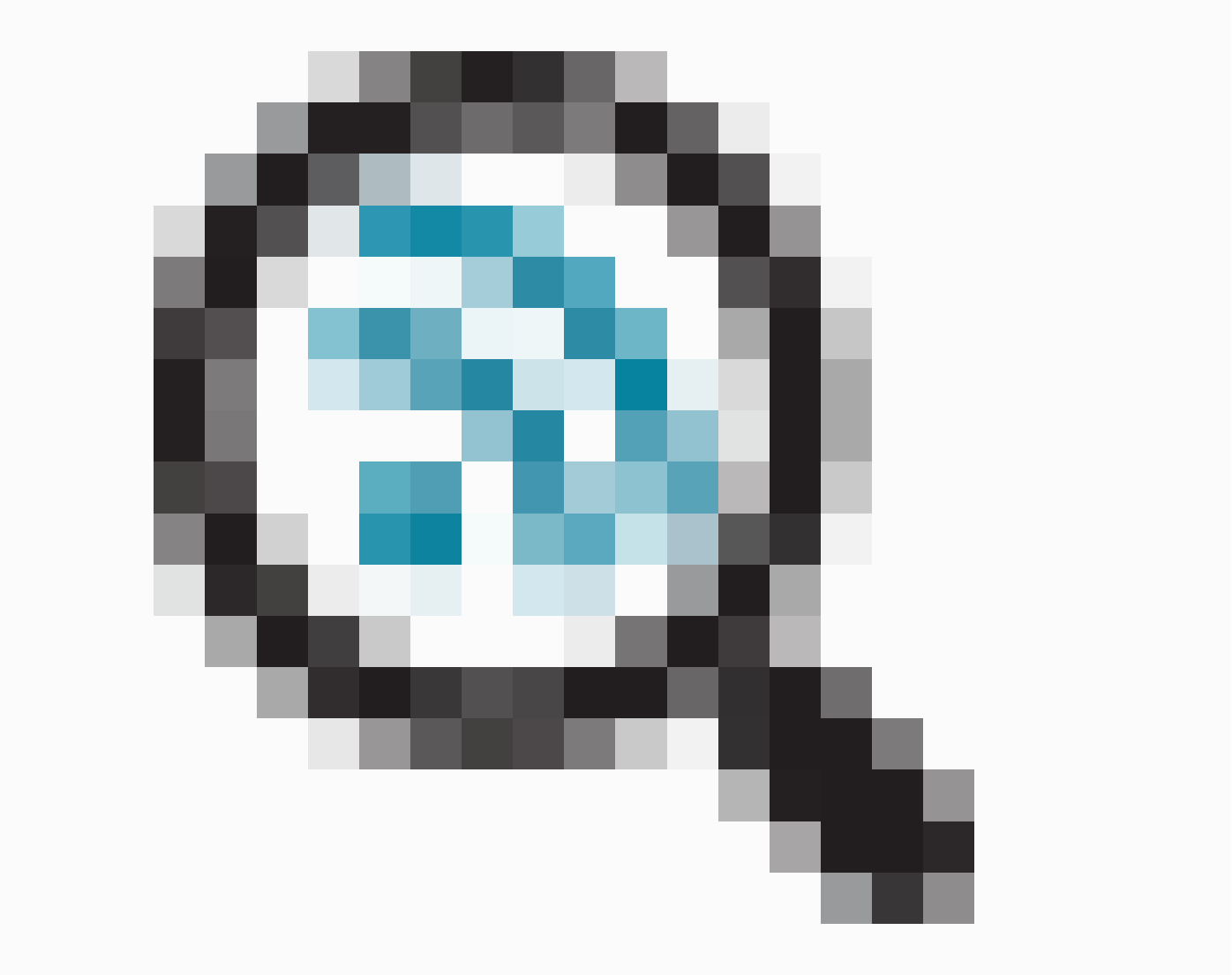
对EAP方法的字典攻击	Y	Y
针对802.1x身份验证的EAP攻击	Y	Y
检测到虚假AP	Y	Y
检测到假DHCP服务器	n	Y
检测到FAST WEP裂纹工具	Y	Y
分段攻击	Y	Y
检测到Honeypot AP	Y	Y
检测到Hotspotter工具	n	Y
广播帧不正确	n	Y
检测到格式错误的802.11数据包	Y	Y
中间人攻击	Y	Y
检测到Netstumbler	Y	Y
检测到Netstumbler受害者	Y	Y
检测到PSPF违规	Y	Y
检测到软AP或主机AP	Y	Y
检测到伪造MAC地址	Y	Y
检测到可疑的非工作时间流量	Y	Y
按供应商列表进行未经授权的关联	n	Y
检测到未经授权的关联	Y	Y
已检测到Wellenreiter	Y	Y

注意：添加CleanAir还将启用对非802.11攻击的检测。

图11 - WCS wIPS简档视图



在图11中，配置来自WCS的wIPS配置文件，该图标表示仅在AP位于MM中时才会检测到攻击，而在ELM中时仅会尽力而为



。

排除ELM故障

检查以下项目：

- 确保配置了NTP。
- 确保MSE时间设置采用UTC。
- 如果设备组不工作，请将重叠配置文件SSID与Any一起使用。重新启动AP。
- 确保已配置许可（当前ELM AP使用KAM许可证）
- 如果wIPS配置文件更改过于频繁，请再次同步MSE控制器。确保配置文件在WLC上处于活动状态。
- 使用MSE CLI确保WLC是MSE的一部分：
    1. 通过SSH或telnet连接到您的MSE。
    2. Execute /opt/mse/wips/bin/wips_cli — 此控制台可用于访问以下命令，以收集有关自适

应wIPS系统状态的信息。

3. show wlc all — 在wIPS控制台内发出。此命令用于验证与MSE上的wIPS服务主动通信的控制器。请参阅图 12。

   图12 - MSE CLI使用MSE wIPS服务验证WLC是否处于活动状态

```
<#root>

wIPS>

show wlc all


WLC MAC               Profile             Profile
Status                   IP
Onx Status Status
-----------------------------------------------
-----------------------------------------------
----
00:21:55:06:F2:80    WCS-Default         Policy
active on controller     172.20.226.197
Active
```

- 确保使用MSE CLI在MSE上检测到警报。
  - show alarm list — 在wIPS控制台内发出。此命令用于列出wIPS服务数据库中当前包含的警报。密钥字段是分配给特定警报的唯一散列密钥。Type字段是警报的类型。图13中的此图表显示了警报ID列表和说明：

    图13 - MSE CLI show alarm list命令

```
<#root>

wIPS>

show alarm list


Key         Type  Src MAC
LastTime               Active          First Time
-----------------------------------------------
-----------------------------------------
89          89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631       95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183     99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

    First Time和Last Time字段表示检测到警报的时间戳；这些时间戳以UTC时间存储。如果当前检测到警报，则Active字段会突出显示。

- 清除MSE数据库。
    - 如果您遇到了MSE数据库已损坏的情形，或者没有其他故障排除方法可工作，则最好清除数据库并重新开始。

      图14 - MSE services命令

```
1. /etc/init.d/msed stop
2. 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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。