在无线局域网控制器(WLC)和无线控制系统(WCS)的基于规则的恶意分类

目录

简介

在无线控制系统(WCS) 5.0版本中， WCS提高了不同的非法AP类型的恶意管理功能和，假设用户定义的规则自动地分类恶意AP。WCS应用非法AP分类规则到控制器。本文解释增强版歹徒管理功能和必要步骤配置在无线局域网控制器(WLC)和WCS的此功能。

先决条件

要求

Cisco 建议您了解以下主题：

- 知识轻量级接入点协议 (LWAPP)
- 无线局域网控制器安全问题解决方案知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件5.2的Cisco 4400系列WLC
- Cisco Aironet 1130 AG系列轻量级接入点(拉普)
- 思科无线控制系统版本5.2

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。

基于规则的恶意分类

在版本5.0之前的WCS版本中， WCS显示许多非法接入点(AP)在**安全汇总页**。即使无赖国家有所不同，他们全都出现在一个页，排序由歹徒的BSSID/MAC地址。

在WCS 5.0版本中， WCS提高了恶意管理功能并且介绍新的术语(未保密，有恶意和友好)不同的非法AP类型的和，假设用户定义的规则自动地分类恶意AP。WCS应用非法AP分类规则到控制器。

一旦歹徒的状态手工更改对*外部*， WCS提高无赖国家管理功能保持无赖国家作为*外部*。当WCS拉或处理从其他控制器时的陷阱消息WCS也更新其他控制器的*外部*状态。

为了支持此功能， WLC和WCS应该运行5.0版本。

基于规则的恶意分类术语

使用此新建的功能，这些新建的非法AP类型介绍：

- **有恶意的AP** ：匹配用户定义的有恶意的规则或从友好AP手工移动的检测的AP。
- **友好AP** ：已知的存在，确认，并且托拉斯缺失无赖国家分类如友好。另外，匹配的检测的AP用户定义的友好规则分类如友好。友好AP不可能包含。
- **未保密的AP** ：没有匹配有恶意或友好规则的检测的AP。未保密的AP可以包含。未保密的AP可以手工移动向友好由用户。用户定义的规则自动地移动未保密的AP向友好或有恶意，例如，在检测， SSID是空的。在下恶意报告，找到SSID，并且结果是一用户配置的SSID。

恶意分类规则

这些是分类规则可适用对其中每一个非法AP类型：

- 有恶意的规则匹配管理了SSID匹配用户配置的SSID在SSID的不加密最低RSSI时间持续时间客户端编号关联
- 友好规则托管型SSID用户配置的SSID
- 未保密的规则不匹配有恶意或友好规则

用户能选择根据每个规则匹配**所有，其中任一**或者**某些**规则条件：

- **所有**平均值匹配所有规则的已配置的条件。
- **所有**平均值匹配其中任一个规则的已配置的条件。
- **一些**平均值匹配少量规则的已配置的条件

例如，根据*有恶意的规则*，用户配置*托管型SSID*和*最低RSSI*。然后，用户有匹配的选择**所有**或其中**任一**两个条件，或者请匹配*最低RSSI*情况。

当控制器收到恶意报告时，执行此：

- 检查检测的AP是否在用户配置的MAC列表。如果那样，请分类AP作为一个友好类型。
- 如果检测的AP不在列表，开始运用规则。
- 首先，它运用*有恶意的规则*。如果*有恶意的规则*配比，它分类作为有恶意的类型。如果RLDP/rogue探测器确定此歹徒是在网络，指示无赖国家作为**威胁**。更改无赖国家对**包含的**用户能手工包含AP。如果AP不在网络，指示无赖国家作为**警报**，并且用户能手工包含它。
- 如果*有恶意的规则不*配比，请运用*友好规则*。如果*友好规则*配比，则请分类它作为一个友好类型。
- 如果*友好规则不*配比，请分类此AP如未保密。如果RLDP/rogue探测器确定此歹徒是在网络，请标记无赖国家作为**威胁**并且分类它作为一个有恶意的类型。更改无赖国家对**包含的**用户能手工包含AP。如果AP不在网络，请标记无赖国家作为**警报**，并且用户能手工包含它。
- 用户能手工移动AP向一个不同的分类类型。

恶意分类和无赖国家

此表显示歹徒和无赖国家的不同的分类每个分类的。

基于规则的分类类型	**无赖国家**
有恶意的AP	包含的提醒的威胁包含等待已经删除
未保密的AP	包含的警报包含等待已经删除
友好AP	内部(当前知道)外部(当前请确认)内部缺少(缺失的托拉斯)警报

无赖国家解释

- **等待—**在第一检测，检测的AP在待定状态放置3分钟。这次是满足为了管理的AP能确定检测的AP是否是邻居AP。
- **警报—**在3分钟超时之后，如果不在邻接列表或用户配置的友好MAC列表，检测的AP移动**警告**。
- **威胁—**检测的AP在网络被找到。
- **包含—**检测的AP包含。
- **包含等待—**检测的AP被标记包含，但是遏制操作延迟由于不可用资源。
- **内部—**检测的AP是在网络里面，并且用户手册配置它如**友好，内部**，例如，在实验室网络的AP。
- **外部—**检测的AP是网络的外部，并且用户手册配置它如**友好，外部**，例如，属于相邻的网络的AP。
- **缺失的委托—**如果用户配置的友好MAC检测和听不到在托拉斯超时持续时间，友好AP的无赖国家被标记作为缺失的委托。
- **已经删除—**如果有恶意或未保密的AP没收到所有恶意超时持续时间的控制器的来信， AP的无赖国家被标记作为**已经删除**。

如何配置在WLC的恶意规则

为了配置在无线局域网控制器的恶意规则，请完成这些步骤。

1. 恶意规则可以创建从WLC从**安全>无线保护策略>歹徒策略>歹徒规则**页。

2. 为了创建一项新的恶意策略，请点击**添加规则**按钮。***歹徒规则***窗口出现。输入一名称对于规则。此示例使用Rule1。选择规则种类。这是一个有恶意的规则的示例。单击 **Add**。Rule1创建。
3. 为了编辑此规则，请点击创建的规则。**恶意规则> Edit**页出版。在此页，请检查**Enable (event)规则**复选框启动规则。选择根据需求和其他情况的匹配操作类型正如在此示例。
4. 这是友好恶意规则策略的示例。
5. 恶意规则的输出能被看到在**监视器>欺诈>有恶意的AP**。
6. 同样地，*友好规则*和*未保密的规则的*输出可以查看在**监视器>欺诈>未保密的AP**和**监视器>欺诈>友好AP**页，分别。

如何配置在WCS的恶意规则

恶意规则列表：WCS提供系统层恶意规则设置。为了配置在WCS的恶意规则，请完成这些步骤。

1. 选择**配置>控制器模板**，然后单击**安全>非法AP规则**访问非法AP规则列表页。
2. 单击**增加**在正确顶部下拉菜单添加的**分类规则**一个新的分类规则。
3. 点击模板名称编辑恶意规则。此规则详细信息页使您编辑，更新非法AP规则或者删除规则。**设置参数的非法AP规则：**在此页，当他们检查复选框连接任一或所有这些情况时，用户能启用所有情况：不加密匹配托管型AP匹配用户配置的SSID最低RSSI持续时间最小数量的恶意客户端这是一个有恶意的规则的示例：这是一个友好规则的示例：
4. 非法AP规定页列出创建的所有规则。
5. 下一步是配置规则组和适用于这些规则控制器。为了这，使用在WCS的**非法AP规则**组设置。
6. 为了创建新规则组，请选择**配置>控制器模板**，然后单击**安全>非法AP**从WCS GUI的**规则组**。
7. 非法AP规则Groups>新建的模板页启用您添加，更新非法AP规则组，删除规则，并且适用于规则组控制器。请使用添加/删除按钮选择此规则组的非法AP规则。请使用Up/Down按钮指定规则应用的命令。示例如下。一旦规则组配置，请点击**"Save"**。
8. 一旦救规则组，它可以应用到控制器。为了适用于规则组控制器，请编辑规则组。点击规则组名。单击**适用于控制器**。在Next页，请选择此规则应用的控制器。示例如下。
9. 一旦规则应用到控制器，您看到在WCS的一个**成功消息**。
10. 关于分级AP的详细信息在**安全汇总页**可以查看。示例如下。
11. 当您点击从安全汇总页时的适当的分类关于分级AP的详细信息，特别地有恶意，友好和未保密的AP，可以查看。这是有恶意的AP的一示例。

相关信息

- 统一无线网络的恶意检测
- 技术支持和文档 - Cisco Systems