WAP121和WAP321接入点上的欺诈接入点 (AP)检测

目标

非法接入点(AP)是未经系统管理员明确授权而安装在网络上的接入点。非法接入点会带来安全 威胁,因为任何有权访问该区域的人都可能有意或无意地安装无线接入点,以允许未经授权的 人员访问网络。"恶意AP检测"页显示有关这些接入点的信息。您可以将任何授权接入点添加到 受信任AP列表。本文介绍如何在WAP121和WAP321接入点上检测欺诈接入点(AP)

适用设备

·WAP121 · WAP321

软件版本

•1.0.3.4

欺诈AP检测配置

步骤1.登录到接入点配置实用程序并选择Wireless > Rogue AP Detection。将打*开"欺诈AP*检 测"页:

Rogue AP Detection
Refresh
AP Detection: Enable
Save

步骤2.选中Enable以启用AP检测。

Rogue AP D	etection
Refresh	
AP Detection:	Enable
Save	

步骤3.在启用AP检测后,单击Save以显示检测到的恶意接入点列表。系统将显示警告屏幕。





步骤4.单击"确定"继续。如下所示显示Detected Rogue AP列表。

Detected Rogu	e AP List												
Action	MAC Address	Beacon Interval (milliseconds)	Туре	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Trust	使于改动动力	102	AP	(mex) (sump)	Off	Off	2.4	1	1	al	5	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,
Trust	使用语言的	102	AP	(inter) (State)	Off	Off	2.4	1	1	0	3	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,
Trust	100106-56-58-801-68	100	AP	(Non Broadcasting)	On	Off	2.4	1	1	0	5	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,
Trust	00.003608/0	100	AP	(Non Broadcasting)	On	Off	2.4	1	1	_ oOQ	3	Fri Dec 31 12:00:02 1999	1,2,5.5,6,9,11,
Trust	0100000000000	102	AP	(MNRA / SECOND	On	On	2.4	1	1	0	6	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,
Trust	1814 (mail: 1817) (m	102	AP	ANRA (Sama)	Off	Off	2.4	1	1	0	5	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,
Trust	at 18 Proceeding	102	AP	Anne (same	Off	Off	2.4	1	1		4	Fri Dec 31 12:00:04 1999	1,2,5.5,6,9,11,

显示检测到的接入点的以下信息:

·MAC地址 — 检测到的AP的MAC地址。

·信标间隔(毫秒) — 被检测AP使用的信标间隔。信标帧由AP定期传输,以通告无线网络 的存在。发送信标帧的默认时间为每100毫秒发送一次。

- ·类型 检测到的设备的类型。可以是AP或对等。
- ·SSID 检测到的AP的SSID。
- ·隐私 指示相邻AP上是否存在任何安全。
- ·WPA 指示检测到的AP的WPA安全性是关闭还是打开。
- ·频段 表示在检测到的AP上使用的IEEE 802.11模式。可以是2.4或5。
- ·信道 检测到的AP当前广播的信道。
- ·速率 检测到的AP当前广播的速率。
- ·信号 从检测到的AP发射的无线电信号的强度。
- ·信标 自首次检测到AP以来从AP接收的信标总数。
- ·最后信标 从检测到的AP接收的最后信标的日期和时间。
- ·速率 检测到的AP的支持和基本速率集(以兆位/秒为单位)。

Detected Rog	ue AP List
Action	MAC Address
Trust	
Trust	
Trust	

,并可以将当前列表保存到您的PC,以便下载/备份转到"下载/备份受信任<u>AP列表"</u>。

Trusted AP List							
Action	MAC Address	Туре	SSID	Privacy	Band	Channel	
Untrust	(4-4-98-8-76-9	AP	PROVIDE WARD +1	Off	2.4	4	

步骤6.(可选)如果要删除受信任AP列表,请单击Untrust。

下载/备份受信任AP列表

Save Action:	 Download (PC to AP) Backup (AP to PC)
Source File Name:	Browse No file selected.
File Management Destination:	Replace Merge

步骤1.选择是从PC下载当前受信任AP列表,还是从Save Action(保存操作)将当前列表保存 到PC。

·下载(PC到AP) — 如果要从文件导入列表并替换已知AP列表的内容,请转到<u>下载(PC到</u> <u>AP)</u>。

·备份(AP到PC) — 如果要将当前列表保存到PC,请转到备份(AP<u>到PC)</u>。

下载(PC到AP)

Download/Backup Trusted AP	List
Save Action:	 Download (PC to AP) Backup (AP to PC)
Source File Name:	Browse Eaxmple_test.txt
File Management Destination:	 Replace Merge
Save	

步骤1.单击"下载(PC到AP)"单选按钮从PC下载列表。

步骤2.单击**Browse**以在PC上找到文件。导入文件应是扩展名为.txt或.cfg的纯文本文件。导入 文件中的条目是十六进制格式的MAC地址,每个二进制八位数用冒号分隔。条目必须用一个 空格分隔。文件必须仅包含MAC地址,然后AP接受该文件。

步骤3.选择File Management Destination以替换或将内容添加到受信任AP列表。

·替换 — 导入列表并替换受信任AP列表的内容

·合并——导入导入文件的AP并将其添加到受信任AP列表。

注意:导入完成后,屏幕刷新,导入文件中AP的MAC地址显示在Known AP List(已知AP列 表)中。

步骤4.单击"保存"以保存所做的所有更改。

备份(AP到PC)

o

Download/Backup	Trusted AP List	
Save Action:	 Download (PC to AP) Backup (AP to PC) 	
Save		

步骤1.单击"备份(AP到PC)"单选按钮将列表保存到PC。

步骤2.单击Save以保存所做的更改,然后出现通知窗口,如下所示,其中提供了文件的信息

	Opening Rogue2.cfg	L
You have chosen to	open:	
Rogue2.cfg		
which is: Text	Document	
from: http://1	92.168.1.245	
What should Firefo	x do with this file?	
O Open with	Notepad (default)	
Save File		
Do this <u>a</u> uto	matically for files like this from now on. OK Cance	