目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[Cisco Unified无线网络安全问题解决方案](#)
[无线局域网控制器Layer2 ？第3层安全兼容性矩阵](#)
[相关信息](#)

简介

本文为支持的Layer2和第3层安全机制提供兼容性矩阵在无线局域网控制器(WLC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解轻量 AP 和 Cisco WLC 配置方面的基础知识
- 了解轻量 AP 协议 (LWAPP) 的基础知识
- 无线安全解决方案基础知识

使用的组件

运行固件版本7.0.116.0的本文档中的信息根据一Cisco 4400/2100系列WLC

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。

Cisco Unified无线网络安全问题解决方案

Cisco Unified无线网络支持Layer2和第3层安全方法。

- 第2层安全
- 第3层安全(WLAN)或第3层安全(访客LAN)

访客LAN不支持第2层安全。

列出支持此表无线局域网控制器不同的层2和第3层安全方法。这些安全方法可以从在WLAN的**WLAN > Edit**页的**安全选项卡**启用。

第2层安全机制		
参数		**说明**
第2层安全	无	没有选择的第2层安全。
	WPA+WPA2	请使用此设置为了启用wi-fi受保护的访问。
	802.1X	请使用此设置为了启用802.1x验证。
	静态 WEP	请使用此设置为了启用静态WEP加密。
	静态WEP + 802.1x	请使用此设置为了启用静态WEP和802.1x参数。
	CKIP	请使用此设置为了启用思科锁上完整性协议(CKIP)。功能在AP型号1100， 1130和不是1200，但是AP1000。要使此功能正常运行，需要启用Aironet IE。CKIP 将加密密钥扩展到 16 字节。
MAC过滤	选择由MAC地址过滤客户端。请由在MAC过滤器>New页的MAC地址本地配置客户端。否则，请配置RADIUS服务器的客户端。	
第3层安全机制(WLAN)		
参数		**说明**
第3层安全	无	没有选择的第3层安全。
	IPsec	请使用此设置为了启用IPSec。在您实现IPSec前，您需要检查软件可用性和客户端硬件兼容性。 **注意：** 您必须安排可选VPN/Enhanced安全模块(crypto处理器卡)安装启用IPSec。验证它安装在您的在库存页的控制器。
	VPN通过	请使用此设置为了启用VPN通过。 **注意：** 此选项不是可用的在Cisco 5500系列控制器和Cisco 2100系列控制器。然而，使用ACL，您能通过创建一开放WLAN复制在一个Cisco 5500系列控制器或Cisco 2100系列控制器的此功能。
Web策	选择此复选框启用Web策略。控制器到/从无线客户端转发DNS流量在验证前。	

略	**注意：** Web策略不可能使用与IPsec或VPN通过选项的组合。 这些参数显示： • 验证？如果选择此选项，提示用户输入用户名和密码，当连接无线网络的时客户端。 • Passthrough ？如果选择此选项，用户能访问网络直接地，不用用户名和密码验证。 • 有条件的Web重定向？如果选择此选项，用户可以有条件地重定向到一个特定的网页，在802.1X验证成功地完成后。您可以在您的RADIUS 服务器上指定重定向页以及发生重定向的条件。 • 飞溅页Web重定向？如果选择此选项，用户重定向对一个特定的网页，在802.1X验证成功地完成后。在重定向，用户有对网络后的完全权限。您能指定在您的RADIUS服务器的飞溅网页。 • 在MAC过滤器失败？Enable (event) Web验证MAC过滤器失败。
预先身份验证ACL	选择将用于客户端和控制器之间的流量ACL。
改写全局配置	如果选择验证，显示。检查此方框为了改写在Web登录页设置的全局身份验证配置。
Web认证类型	如果选择Web策略并且改写全局配置，显示。选择Web验证的类型： • 内部 • 定制(下载) 登录页？选择从下拉列表的登录页。登录失败页？选择显示给客户端的登录页，如果Web验证发生故障。logout页？选择显示给客户端，当用户登录在系统外面时的登录页。 • 外部(请重定向到外部服务器) URL ？输入外部服务器的URL。
给输入发电子邮件	如果选择Passthrough，显示。如果选择此选项，提示对于您的电子邮件地址，当连接对网络时。

第3层安全机制(访客LAN)		
参数		**说明**
第3层安全	无	没有选择的第3层安全。
	Web 身份验证	如果选择此选项，提示对于用户名和密码，当连接网络的时客户端。
	Web Passthrough	如果选择此选项，您能访问网络直接地，不用用户名和密码验证。
预先身份验证ACL		选择将用于客户端和控制器之间的流量ACL。
改写全局配置		检查此方框为了改写在Web登录页设置的全局身份验证配置。
Web认证类型		如果选择改写全局配置，显示。选择Web验证的类型： • 内部 • 定制(下载) 登录页？选择从下拉列表的登录页。登录失败页？选择显示给客户端的登录页，如果Web验证发生故障。logout页？选择显示给客户端，当用户登录在系统外面时的登录页。 • 外部(请重定向到外部服务器) URL ？输入外部服务器的URL。
给输入发电子邮件		如果选择Web Passthrough，显示。如果选择此选项，提示对于您的电子邮件地址，当连接对网络时。

注意： 在控制器软件版本4.1.185.0或以上， CKIP支持为仅使用与静态WEP。它不支持为了用在动态WEP上。所以，配置以动态WEP使用CKIP的无线客户端无法联合到为CKIP配置的无线局域网。思科建议您使用动态WEP，不用(是安全的较少)的CKIP或与的WPA/WPA2是安全的更多)的TKIP或AES (。

无线局域网控制器Layer2 ？第3层安全兼容性矩阵

当您配置在无线局域网的安全，时Layer2和第3层安全方法可以用于联合。然而，不是所有的第2层安全方法可以与所有第3层安全方法一起使用。显示支持此表无线局域网控制器Layer2和第3层安全的兼容性矩阵方法。

第2层安全机制	第3层安全机制	兼容性
无	无	有效

WPA+WPA2	无	有效
WPA+WPA2	Web 身份验证	无效
WPA-PSK/WPA2-PSK	Web 身份验证	有效
WPA+WPA2	Web Passthrough	无效
WPA-PSK/WPA2-PSK	Web Passthrough	有效
WPA+WPA2	有条件的Web重定向	有效
WPA+WPA2	飞溅页Web重定向	有效
WPA+WPA2	VPN Passthrough	有效
802.1x	无	有效
802.1x	Web 身份验证	无效
802.1x	Web Passthrough	无效
802.1x	有条件的Web重定向	有效
802.1x	飞溅页Web重定向	有效
802.1x	VPN Passthrough	有效
静态 WEP	无	有效
静态 WEP	Web 身份验证	有效
静态 WEP	Web Passthrough	有效
静态 WEP	有条件的Web重定向	无效
静态 WEP	飞溅页Web重定向	无效
静态 WEP	VPN Passthrough	有效
Static-WEP+802.1x	无	有效
Static-WEP+802.1x	Web 身份验证	无效
Static-WEP+802.1x	Web Passthrough	无效
Static-WEP+802.1x	有条件的Web重定向	无效
Static-WEP+802.1x	飞溅页Web重定向	无效
Static-WEP+802.1x	VPN Passthrough	无效
CKIP	无	有效
CKIP	Web 身份验证	有效
CKIP	Web Passthrough	有效
CKIP	有条件的Web重定向	无效
CKIP	飞溅页Web重定向	无效
CKIP	VPN Passthrough	有效

相关信息

- 无线 LAN 控制器和轻量接入点基本配置示例
- 轻量 AP (LAP) 注册到无线 LAN 控制器 (WLC)
- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- 无线局域网控制器(WLC)常见问题
- 技术支持和文档 - Cisco Systems