WLC第2层和第3层安全兼容性矩阵

目录

简介

本文档提供无线局域网控制器(WLC)上支持的第2层和第3层安全机制的兼容性矩阵。

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

本文档中的信息基于运行固件版本7.0.116.0的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。

思科统一无线网络安全解决方案

思科统一无线网络支持第2层和第3层安全方法。

- 第2层安全
- 第3层安全（适用于WLAN）或第3层安全（适用于访客LAN）

访客LAN不支持第2层安全。

下表列出了无线LAN控制器支持的各种第2层和第3层安全方法。可以从WLAN的**WLANs > Edit**页上的**Security**选项卡启用这些安全方法。

第2层安全机制		
参数		**描述**
第2层安全	无	未选择第2层安全。
	WPA+WPA2	使用此设置可启用Wi-Fi保护访问。
	802.1X	使用此设置以启用802.1x身份验证。
	静态WEP	使用此设置可启用静态WEP加密。
	静态WEP+802.1x	使用此设置可同时启用静态WEP和802.1x参数。
	CKIP	使用此设置可启用思科密钥完整性协议(CKIP)。在AP型号1100、1130和1200上正常工作，但在AP 1000上不起作用。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	选择以按MAC地址过滤客户端。在MAC Filters > New页面中按MAC地址本地配置客户端。否则，请在RADIUS服务器上配置客户端。	
第3层安全机制（适用于WLAN）		
参数		**描述**
第3层安全	无	未选择第3层安全。
	IPsec	使用此设置以启用IPSec。在实施IPSec之前，您需要检查软件可用性和客户端硬件兼容性。 **注意：**必须安装可选的VPN/增强型安全模块（加密处理器卡）才能启用IPSec。在Inventory（资产）页面上，验证它是否安装在您的控制器上。
	VP	使用此设置以启用VPN直通。

	N直通	**注意：**此选项在Cisco 5500系列控制器和Cisco 2100系列控制器上不可用。但是，通过使用ACL创建开放式WLAN，您可以在Cisco 5500系列控制器或Cisco 2100系列控制器上复制此功能。
Web策略	选中此复选框可启用Web策略。控制器在身份验证之前将DNS流量转发到无线客户端或从无线客户端转发DNS流量。 **注意：**Web策略不能与IPsec或VPN直通选项结合使用。 将显示以下参数： • Authentication — 如果选择此选项，则在将客户端连接到无线网络时，系统会提示用户输入用户名和密码。 • Passthrough — 如果选择此选项，用户可以直接访问网络，无需用户名和密码身份验证。 • 条件网络重定向(Conditional Web Redirect) — 如果选择此选项，则在802.1X身份验证成功完成之后，用户可以有条件重定向到特定网页。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。 • Splash Page Web Redirect — 如果选择此选项，则在802.1X身份验证成功完成后，用户将被重定向到特定网页。在重定向后，用户具有对网络的完全访问权限。您可以在RADIUS服务器上指定启动网页。 • On MAC Filter failure — 启用Web身份验证MAC过滤器故障。	
预身份验证ACL	选择要用于客户端和控制器之间流量的ACL。	
超载全局配置	如果选择Authentication，则显示。选中此框以覆盖Web登录页面上设置的全局身份验证配置。	
Web身份验证类型	如果选择Web Policy和Over-ride Global Config，则显示。选择一种Web身份验证类型： • 内部 • 定制（已下载）Login Page — 从下拉列表中选择登录页。“登录失败”(Login Failure)页面 — 选择在Web身份验证失败时显示给客户端的登录页面。注销页面 — 选择当用户注销系统时显示给客户端的登录页面。 • 外部（重定向到外部服务器）URL — 输入外部服务器的URL。	
电邮输入	如果选择“直通”，则显示。如果选择此选项，则在连接到网络时，系统会提示您输入电子邮件地址。	
第3层安全机制（用于访客LAN）		

参数		描述
第3层安全	无	未选择第3层安全。
	Web身份验证	如果选择此选项，则在将客户端连接到网络时，系统会提示您输入用户名和密码。
	网络直通	如果选择此选项，可以直接访问网络，无需用户名和密码身份验证。
预身份验证ACL		选择要用于客户端和控制器之间流量的ACL。
超载全局配置		选中此框以覆盖Web登录页面上设置的全局身份验证配置。
Web身份验证类型		如果选择Over-ride Global Config，则显示。选择一种Web身份验证类型： • 内部 • 定制（已下载）Login Page — 从下拉列表中选择登录页。“登录失败”(Login Failure)页面 — 选择在Web身份验证失败时显示给客户端的登录页面。注销页面 — 选择当用户注销系统时显示给客户端的登录页面。 • 外部（重定向到外部服务器）URL — 输入外部服务器的URL。
电邮输入		如果选择Web直通，则显示。如果选择此选项，则在连接到网络时，系统会提示您输入电子邮件地址。

注意：在控制器软件版本4.1.185.0或更高版本中，仅支持将CKIP与静态WEP配合使用。不支持将其用于动态WEP。因此，配置为将CKIP与动态WEP配合使用的无线客户端无法与为CKIP配置的无线LAN关联。Cisco建议您使用不带CKIP的动态WEP（不太安全）或带TKIP或AES的WPA/WPA2（更安全）。

无线LAN控制器第2层 — 第3层安全兼容性矩阵

在无线LAN上配置安全时，可以同时使用第2层和第3层安全方法。但是，并非所有第2层安全方法都可用于所有第3层安全方法。下表显示了无线LAN控制器上支持的第2层和第3层安全方法的兼容性矩阵。

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	网络直通	无效

WPA-PSK/WPA2-PSK	网络直通	有效
WPA+WPA2	有条件的Web重定向	有效
WPA+WPA2	启动页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	网络直通	无效
802.1x	有条件的Web重定向	有效
802.1x	启动页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	网络直通	有效
静态 WEP	有条件的Web重定向	无效
静态 WEP	启动页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	网络直通	无效
Static-WEP+ 802.1x	有条件的Web重定向	无效
Static-WEP+ 802.1x	启动页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	网络直通	有效
CKIP	有条件的Web重定向	无效
CKIP	启动页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

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）。