在WLC上配置Web身份验证代理

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>WLC上的Web身份验证代理</u> <u>在WLC上配置Web身份验证代理</u> 配置 <u>验证</u> 相关信息

简介

本文档提供在无线局域网控制器(WLC)上使用Web身份验证代理功能的配置示例。

先决条件

要求

尝试进行此配置之前,请确保满足以下要求:

- •了解轻量接入点(LAP)和思科WLC的配置。
- •了解轻量接入点协议(LWAPP)/无线接入点的控制和调配(CAPWAP)。
- •具有Web身份验证知识。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件版本 7.0.116.0 的 Cisco 4400 WLC
- Cisco 1130AG系列LAP
- •运行固件版本4.2的思科802.11a/b/g无线客户端适配器

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

有关文档约定的更多信息,请参考 <u>Cisco 技术提示约定。</u>

WLC上的Web身份验证代理

本文档假设读者事先了解网络身份验证以及在思科WLC上配置Web身份验证所涉及的步骤。如果您 是新用户,请阅读以下详细介绍Web身份验证过程的文档:

- 无线局域网控制器 Web 身份验证配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除

Web身份验证代理功能随WLC版本7.0.116.0引入。

Web浏览器具有三种可由用户配置的Internet设置:

- 自动检测
- 系统代理
- 手动

此功能使在浏览器中启用了手动Web代理的客户端能够使用控制器进行Web身份验证。

在配置为Web身份验证的网络中,如果客户端配置为手动代理设置,则控制器不会侦听此类代理端 口,因此客户端将无法与控制器建立TCP连接。实际上,用户无法访问任何登录页面进行身份验证 和访问网络。

当客户端请求启用了Web身份验证代理功能的任何URL时,控制器以网页进行响应,提示用户更改 Internet代理设置以自动检测代理设置。

此过程可防止浏览器的手动代理设置丢失。配置此功能后,用户可以通过Web身份验证策略访问网 络。

默认情况下,为端口80、8080和3128提供此功能,因为这些端口是Web代理服务器最常用的端口 。

在WLC上配置Web身份验证代理

本部分提供有关如何配置本文档所述功能的信息。

配置

完成以下步骤,以使用控制器GUI配置Web身份验证代理:

- 1. 从控制器GUI中,选择Controller > General。
- 2. 要启用WebAuth代理,请从WebAuth代理重定向模式下拉列表中选择启用。

cisco	MONITOR WLANS CONTROLLE	R WIRELESS SECURITY	MANAGEMENT
Controller	General		
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Name 802.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicast Mode Å AP Fallback Apple Talk Bridging Fast SSID change Default Mobility Domain Name RF Group Name User Idle Timeout (seconds) ARP Timeout (seconds) Web Radius Authentication 802.3 Bridging Operating Environment Internal Temp Alarm Limits	WLC-4400 Disabled • Disabled • Unicast • Enabled • Disabled • Disabled • WLAN-LAB WLAN-LAB WLAN-LAB 300 300 PAP • Disabled • Commercial (0 to 40 C) 0 to 65 C	(LAG
	WebAuth Proxy Redirection Mode WebAuth Proxy Redirection Port	Enabled 💌 Disabled Enabled	

 在Web身份验证代理重定向端口文本框中,输入Web身份验证代理的端口号。此文本框包含控制器侦听Web身份验证代理重定向的端口号。默认情况下,假定为三个端口80、8080和 3128。如果将Web身份验证重定向端口配置为除这些值之外的任何端口,则必须指定该值。

cisco		R WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Controller	General	
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server	Name 802.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicest Mode & AP Fallback	WLC-4400 Disabled • (LAG Mode is currently disabled). Disabled • (LAG Mode is currently disabled).
Mobility Management Ports NTP CDP	Apple Talk Bri Fast SSID che Default Mobilit R/F Group Nam	plorer ion will be enabled for proxy ports 80, 8080 and 3128 by default, and for user-configured proxy redirection port if any, et the system for the webAuth proxy setting to take effect.
▶ Advanced	User Idle Tim ARP Timeout (seconds) Web Radius Authentication 802.3 Bridging Operating Environment Internal Temp Alarm Limits WebAuth Proxy Redirection Mode WebAuth Proxy Redirection Port	300 PAP Disabled • Commercial (0 to 40 C) 0 to 65 C Enabled • 0

4. 单击 Apply。

要从CLI配置WebAuth代理,请发出以下命令:

config network web-auth proxy-redirect {enable | disable} 使用**config network web-auth port** *oprt-number*>命令设置Web身份验证端口号。

配置WLC后,保存配置并重新启动控制器以使配置生效。

验证

要查看Web身份验证代理配置的当前状态,请发出**show network summary**或**show running-config**命 令。

(Cisco Controller) >show network summary

RF-Network Name	WLAN-LAB
Web Mode	Disable
Secure Web Mode	Enable
Secure Web Mode Cipher-Option High	Disable
Secure Web Mode Cipher-Option SSLv2	Enable
Secure Shell (ssh)	Enable
Telnet	Enable
Ethernet Multicast Forwarding	Disable
Ethernet Broadcast Forwarding	Disable
AP Multicast/Broadcast Mode	Unicast
IGMP snooping	Disabled
IGMP timeout	60 seconds
IGMP Query Interval	20 seconds
User Idle Timeout	300 seconds
ARP Idle Timeout	300 seconds
Cisco AP Default Master	Disable
AP Join Priority	Disable
Mgmt Via Wireless Interface	Disable
Mgmt Via Dynamic Interface	Disable
Bridge MAC filter Config	Enable
Bridge Security Mode	EAP
More or (q)uit	
Mesh Full Sector DFS	Enable
Apple Talk	Disable
AP Fallback	Enable
Web Auth Redirect Ports	80
Web Auth Proxy Redirect	Enable
Fast SSID Change	Disabled
802.3 Bridging	Disable
IP/MAC Addr Binding Check	Enabled

现在,我们将无线客户端连接到我们为Web身份验证配置的访客SSID。

cisco	Monitor wlans controller wireless security management commands help f
WLANs	WLANs > Edit 'Guest1'
WLANS WLANS	General Security QoS Advanced
Advanced	Profile Name Guesti
	Type WLAN SSID Guest1
	Status I Enabled
	Security Policies Web-Auth (Modifications done under security tab will appear after applying the changes.)
	Radio Policy All
	Interface/Interface Group(G) management •
	Multicast Vian Feature Enabled Broadcast SSID I Enabled

假设您有内部DHCP服务器,客户端将连接到WLAN Guest1并获取IP地址。当客户端尝试访问 URL(例如,www.cisco.com)时,由于客户端浏览器上启用了手动代理,因此使用Web身份验证代 理功能的控制器以网页进行响应,提示用户更改Internet代理设置以自动检测代理设置。

configured with proxy settings
configured with proxy settings
are follow these steps. Internet Options'. Is and click on 'LAN Settings'. 'detect settings' option under Automatic coaffiguration and click OK. try another URL. Opticas'. Stings and click on the 'Network' tab. tron under Connection. my settings for this network' and click OK. try another URL. Close
e m or th

此时,客户端知道需要禁用手动代理设置。在这里,您可以看到如何在Firefox 3.6版上禁用手动代 理设置。

- 1. 在Firefox浏览器中,选择工具 > 选项,然后选择高级。
- 2. 单击Network选项卡,然后选择Settings。

Options							×
General	Tabs	Content	Applications	Privacy	Security	Advanced	
General N	etwork U	pdate Encry	/ption		-		
Connec	tion Ire how Fire	efox connect	ts to the Intern	et		Settings	
Offline S Use up I tel The foll	Storage to 50 I me when owing web	MB of s a web site a: sites have s	pace for the ca sks to store dat tored data for (che a for offline offline use:	use (<u>C</u> lear Now E <u>x</u> ceptions	
						Remove	
				ок (Cancel		

3. 在Connection Settings窗口中,选择Auto-detect proxy settings for this network。

~			-	· · · ·	Contraction of the local division of the loc
L	on	nect	Ion	Sen	ings
	4.24				

) <u>O</u> se system prod) <u>M</u> anual proxy co	nfiguration:		
HTTP Proxy:	X.X.X.X	Port:	8080
	Use this proxy server for all pro	tocols	
<u>S</u> SL Proxy:		Port:	0
ETP Proxy:	1	Po <u>r</u> t:	0 🕻
<u>G</u> opher Proxy:		Port:	0
SO <u>C</u> KS Host:	1	Port:	0
) 50CK5 v4 () 50CK5 v5	-	
No Proxy for:	localhost, 127.0.0.1		
	Example: .mozilla.org, .net.nz, 192.	168,1,0	0/24

完成此操作后,请刷新浏览器并再次尝试访问URL。此时,您将重定向到Web Authentication页面 。客户端可以向您提供凭证,您也可以登录到访客网络。

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name	
Password	
	Submit

相关信息

- 无线局域网控制器 Web 身份验证配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除
- Cisco 无线 LAN 控制器配置指南 7.0.116.0 版
- <u>技术支持和文档 Cisco Systems</u>

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)。