設定WLC上的Web驗證Proxy

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>WLC上的Web驗證代理</u> <u>設定WLC上的Web驗證Proxy</u> <u>組態</u> <u>驗證</u> 相關資訊

簡介

本檔案將提供在無線LAN控制器(WLC)上使用Web驗證代理功能的組態範例。

必要條件

需求

嘗試此組態之前,請確保符合以下要求:

- •瞭解輕量型存取點(LAP)和Cisco WLC的組態。
- 瞭解輕量型存取點通訊協定(LWAPP)/無線存取點控制和布建(CAPWAP)。
- •瞭解Web驗證。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 4400 WLC(執行韌體版本7.0.16.0)
- Cisco 1130AG系列LAP
- 執行韌體版本4.2的Cisco 802.11a/b/g無線使用者端配接器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>

WLC上的Web驗證代理

本檔案假設閱讀器事先瞭解Web驗證以及在Cisco WLC上設定Web驗證所涉步驟。如果您是新使用 者,請閱讀以下文檔,其中詳細介紹了Web身份驗證過程:

- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難

Web驗證代理功能是在WLC 7.0.116.0版中匯入。

Web瀏覽器具有三種可由使用者配置的Internet設定:

- 自動檢測
- 系統代理
- 手動

此功能可讓在瀏覽器中啟用手動Web代理的使用者端更易於使用控制器進行Web驗證。

在設定為Web驗證的網路中,如果使用者端設定為手動代理設定,則控制器不會偵聽此類代理連線 埠,因此使用者端無法與控制器建立TCP連線。實際上,使用者無法訪問任何登入頁面進行身份驗 證和訪問網路。

當客戶端請求任何URL並且啟用了Web驗證代理功能時,控制器以網頁響應,該網頁提示使用者更 改Internet代理設定以自動檢測代理設定。

此過程可防止瀏覽器的手動代理設定丟失。設定此功能後,使用者可以透過Web驗證原則存取網路 。

預設情況下,為埠80、8080和3128提供此功能,因為這些埠是Web代理伺服器最常用的埠。

設定WLC上的Web驗證Proxy

本節提供用於設定本文件中所述功能的資訊。

組態

完成以下步驟,以便使用控制器GUI設定Web驗證代理:

- 1. 在控制器GUI上,選擇Controller > General。
- 2. 若要啟用WebAuth Proxy,請從WebAuth Proxy重新導向模式下拉選單中選擇Enabled。

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 • Disabled • Unicast • Enabled • Disabled • Disabled • 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	

3. 在「WebAuth Proxy重新導向連線埠」文字框中,輸入Web驗證Proxy的連線埠號碼。此文本 框包含控制器偵聽Web驗證代理重新導向的連線埠號碼。預設情況下,假定為三個埠80、 8080和3128。如果將Web驗證重新導向連線埠設定為除了這些值以外的任何連線埠,必須指 定該值。

uluili. cisco		WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	General Name B02.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicast Mode 1 AP Fallback Apple Talk Bri Microsoft Internet Exp Fast SSID che Default Mobilit RF Group Nam User Idle Time ARP Timeout (seconds) Web Radius Authentication B02.3 Bridging Operating Environment Internel Temp Alarm Limits WebAuth Proxy Redirection Port	WLC-4400 Disabled = (LAG Mode is currently disabled). Disabled = (LAG Mode is currently disabled). Disabled = (LAG Mode is currently disabled). Disabled = (Disabled = (Disabled = (Disabled or proxy parts 80, 8080) and 3128 by default, and for user-configured proxy redirection port if any. to the system for the webAuth proxy setting to take effect.

4. 按一下「Apply」。

若要從CLI設定WebAuth Proxy,請發出以下命令:

config network web-auth proxy-redirect {enable | disable} 使用**config network web-auth port** <port-number> 命令設定Web驗證連線埠號碼。

設定WLC後,請儲存組態並重新啟動控制器,以便組態生效。

驗證

若要檢視Web驗證代理配置的當前狀態,請發出**show network summary**或**show running-config**命令。

(Cisco Controller) >show network summary

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

Fast SSID ChangeDisabled802.3 BridgingDisableIP/MAC Addr Binding CheckEnabled

現在,我們將無線客戶端連線到我們為Web身份驗證配置的訪客SSID。

cisco	Monitor wlans controller wireless security management commands help	1
WLANs	WLANs > Edit 'Guest1'	
WLANS WLANS	General Security QoS Advanced	
Advanced	Profile Name Guesti	
	Type WLAN	
	Status R Enabled	
	Security Policies Web-Auth (Modifications done under security tab will appear after applying the changes.)	,
	Radio Policy All	-
	Interface/Interface Group(G) management	
	Broadcast SSID I Enabled	

假設您有內部DHCP伺服器,則客戶端連線到WLAN Guest1並獲取IP地址。當使用者端嘗試存取 URL(例如www.cisco.com)時,由於使用者端瀏覽器上啟用手動代理,因此使用Web驗證代理功能 的控制器會以提示使用者變更Internet代理設定以自動偵測代理設定的網頁來回應。

Bie Edit Yew History Bookmarks Look Help	
🔇 🖂 - C 🗙 🏠 🗋 http://dsco.com/	
Most Visited 🥮 Getting Started 流 Latest Headlines	
Modify proxy configuration	
	Your browser is configured with proxy settings
	To get access to the network, please follow these steps.
	For Internet Explorer:
	 Go to 'Tools' and select 'Internet Options'. View the 'Connections' tab and click on 'LAN Settings'. Select the 'Automatically detect settings' option under Automatic configuration and click OK. Refresh the web page or try another URL.
	For Firstfor:
	 Go to 'Tools' and select 'Optices'. Choose the 'Advanced' settings and click on the 'Network' tab. Click on the 'Settings' button under Connection. Choose 'Auto-detect proxy settings for this aetwock' and click OK. Refresh the web page or try another URL.
	Close

此時,客戶端知道需要禁用手動代理設定。在這裡,您可以看到如何在Firefox 3.6版上禁用手動代 理設定。

- 1. 在Firefox瀏覽器中,選擇Tools > Options,然後選擇Advanced。
- 2. 按一下Network頁籤,然後選擇Settings。

Options							X
General	Tabs	Content	Applications	Privacy	Security	Advanced	
General Ne	etwork U	pdate Encry	/ption		1		
Connect	ion re how Fin	efox connect	ts to the Intern	et		Settings	
Offline S Use up t I <u>I</u> ell The follo	itorage :o 50 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 [⊆lear Now E <u>x</u> ceptions	
						Remove	
					Cancel		

3. 在「連線設定」視窗中,選擇Auto-detect proxy settings for this network。

~			All and the second
Lon	necti	on Se	nngs
A. A. M.			

<u>Manual proxy co</u>	nfiguration:		
HTTP Proxy:	X.X.X.X	Port:	8080
	Use this proxy server for all p	protocols	
<u>S</u> SL Proxy:		P <u>o</u> rt:	0
ETP Proxy:		Port:	0 🕻
<u>G</u> opher Proxy:		Port:	0
SO <u>C</u> K5 Host:		Por <u>t</u> :	0 S
	○ 50CK5 v4 ④ 50CK5 v5		
No Proxy for:	localhost, 127.0.0.1		
	Example: .mozilla.org, .net.nz, 19	92,168,1,	0/24

完成此操作後,請刷新瀏覽器,然後再次嘗試訪問URL。這一次,您將重定向到「Web驗證」頁面。使用者端可以為您提供憑證,您也可以登入訪客網路。

Web Authentication	+	
Lo	ogin	

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

相關資訊

- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難
- 思科無線LAN控制器配置指南7.0.116.0版
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。