Web驗證代理組態範例

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>設定WLC</u> <u>配置PAC檔案</u> <u>建立預先驗證ACL</u> <u>快速修復:配置Web瀏覽器</u> <u>驗證</u> 疑難排解

簡介

本文說明如何設定Web驗證,以便使用代理程式。

必要條件

需求

思科建議您瞭解以下主題:

- 無線LAN控制器基本配置
- Web驗證安全

採用元件

本檔案中的資訊是根據思科無線LAN控制器7.0版及更新版本。

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。

設定

網路管理員在網路上使用代理伺服器時,先將網路流量傳送到代理伺服器,然後由代理伺服器將流 量中繼到網際網路。客戶端和代理伺服器之間的連線可以使用埠80以外的TCP埠進行通訊。此埠通 常是TCP埠3128或8080。預設情況下,Web身份驗證僅偵聽埠80。因此,當HTTP GET離開電腦時 ,它會傳送到代理埠,但會被控制器丟棄。

本節介紹如何設定Web驗證以使用代理程式:

1. 設定思科無線LAN控制器(WLC)以監聽代理連線埠。

2. 設定代理自動組態(PAC)檔案,以直接傳回虛擬IP位址。

3. 建立預先驗證存取控制清單(ACL),以便允許使用者端在Web驗證之前下載PAC檔案。 快速修複方法是,您可以手動設定Web瀏覽器以返回192.0.2.1。

以下各小節將詳細介紹這些流程。

設定WLC

此程式介紹如何將控制器偵聽的連線埠變更為Proxy伺服器偵聽的連線埠。

1. 導覽至Controller > General頁面。

Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled 👻
WebAuth Proxy Redirection Port	8080
1. Multicast is not supported with HREA	P on this platform.

- 2. 在「WebAuth Proxy重新導向連線埠」欄位中,輸入您希望WLC偵聽的連線埠以接受使用者端 重新導向。
- 3. 從WebAuth Proxy Redirection Mode下拉式清單中選擇Disabled或Enabled:

如果選擇「**Disabled**」,則使用者端會顯示在正常的Web驗證頁面上,以進行直通或驗證。因 此,如果您使用代理,則需要將所有客戶端瀏覽器配置為不使用192.0.2.1的代理(或WLC使 用的其他虛擬IP地址)。 請參閱<u>設定Web瀏覽器</u>。

如果您選擇「**Enabled**」,則預設情況下WLC會監聽連線埠80、8080和3128,因此您不需要 在WebAuth Proxy重新導向連線埠文字欄位中輸入這些連線埠。如果使用者端在這些連線埠上 傳送HTTP GET,就會看到要求其將代理設定變更為自動的畫面。

he for her udials footeraus foce flab	
🔄 El - C X 🏠 🗋 Mipuldace.com	4
Plost Visited 🥮 Getting Started 崺 Latest Headines	
Modify proxy configuration +	
	Your browser is configured with proxy settings
	To get access to the network, please follow these steps.
	For Internet Explore:
	Oo to 'Toole' and select 'Internet' Options'. Wave the 'Connections' tab and click on 'LAN Settings'. Select the 'Antonastically detect settings' option under Antonastic configuration and click CIC. Reflexh the web page or try another URL.
	For Fanfox
	 Go to 'Toola' and select 'Optiona'. Choose the 'Advaced' actings and click on the 'Network' tab. Click on the 'Setting' button under Connection. Choose 'Auto-detect proxy setting: for fair setwork' and click OK. Refeels the web page or try another USL.
	Close

4. 儲存組態。

5. 重新啟動控制器。

總而言之,在WebAuth Proxy重新導向連線埠中輸入連線埠號碼,以定義WLC偵聽的連線埠。啟用 重新導向模式時,會將使用者端重新導向到代理設定畫面,並預期動態推送Web代理自動探索 (WPAD)或PAC檔案以進行自動代理組態。如果禁用該功能,則客戶端將重定向到正常Web身份驗 證頁面。

配置PAC檔案

WLC的虛擬IP位址需要傳回「direct」,才能讓Web Auth正確驗證使用者身分。直接表示代理伺服 器不代理請求,並且客戶端具有直接訪問IP地址的許可權。這通常是由代理伺服器管理員在 WPAD或PAC檔案中的代理伺服器上配置的。以下是PAC檔案的配置示例:

```
function FindProxyForURL(url, host) {
     // our local URLs from the domains below example.com don't need a proxy:
     if (shExpMatch(host, "*.example.com"))
     if (shExpMatch(host, "192.0.2.1")) <-- (Line states return 1.1.1 directly)
     {
       return "DIRECT";
     }
     // URLs within this network are accessed through
     // port 8080 on fastproxy.example.com:
     if (isInNet(host, "10.0.0.0", "255.255.248.0"))
     {
       return "PROXY fastproxy.example.com:8080";
     }
     // All other requests go through port 8080 of proxy.example.com.
     // should that fail to respond, go directly to the WWW:
     return "PROXY proxy.example.com:8080; DIRECT";
```

建立預先驗證ACL

在Web驗證服務組識別碼(SSID)上放置預先驗證ACL,以便無線使用者端可以在使用者端登入Web Auth之前下載PAC檔案。預先驗證ACL需要僅允許存取PAC檔案所在的連線埠。對代理埠的訪問使 客戶端無需進行Web驗證即可訪問Internet。

- 1. 導覽至**Security > Access Control List**,以在控制器上建立ACL。
- 2. 建立規則以允許PAC下載埠上的流量在兩個方向上都到達Proxy。

Gene	eral									
Acces	s List Name	ACL1								
Deny	Counters	0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	192.168.0.4 / 255.255.255.255	TCP	Any	8081	Any	Any	0	•
2	Permit	192.168.0.4 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8081	Any	Any	Any	0	•

注意:不允許代理HTTP埠。

3. 在控制器上的WLAN組態中,不要忘記選擇剛建立為預先驗證ACL的ACL。

General	Security	QoS	Advan	ced
Layer 2	Layer 3	AAA	Servers	
Layer 3	Security No	ne 🔻		
Ve We	b Policy			
Auth	entication			
Pass	through			
Con	ditional Web R	edirect		
🔘 Spla	ish Page Web F	Redirect		
On f	MAC Filter failu	re ¹¹		
Preauth	entication ACL	A	CL1 🔻	
Over-rie	de Global Conf	ig 🔲	Enable	

快速修復:配置Web瀏覽器

以下程式介紹如何手動設定例外狀況,以便使用者端Web瀏覽器直接連線到192.0.2.1。

- 1. 在Internet Explorer中,導航到工具> Internet選項。
- 2. 按一下Connections頁籤,然後按一下LAN Settings按鈕。
- 3. 在Proxy server區域中,選中Use a proxy server for your LAN覈取方塊,然後輸入伺服器偵聽的(IP)地址和埠。

nternet Options	8 23
General Security Privacy Content Connections Programs	Advanced
To set up an Internet connection, click Set	tup
Automatic configuration	
Automatic configuration may override manual settings. To en use of manual settings, disable automatic configuration.	sure the
Automatically detect settings	
Use automatic configuration script	
Address	
Proxy server	
Use a proxy server for your LAN (These settings will not a dial-up or VPN connections).	pply to
Address: 192.168.162.10 Port: 8080 Adv	anced
Bypass proxy server for local addresses	
ОК	Cancel
OK Cancel	Apply

4. 按一下「**Advanced**」,然後在「Exceptions」區域中輸入WLC的虛擬IP位址。

\$a	Туре	Proxy address to use	Port
	HTTP:	192.168.162.10	:
	Secure:		:
	ETP:		:
	Socks:		:
Except	Use the	e same proxy server for all proto	cols
Except	<u>U</u> se the ions Do <u>n</u> ot us	e same proxy server for all proto e proxy server for addresses beg	cols ginning with:
Except	Use the ions Do not us	e same proxy server for all proto e proxy server for addresses beg	cols

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。