Webauthentifizierungsproxy auf einem WLC konfigurieren

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Webauthentifizierungsproxy auf einem WLC Webauthentifizierungsproxy auf einem WLC konfigurieren Konfigurationen Überprüfung Zugehörige Informationen

Einleitung

Dieses Dokument enthält ein Konfigurationsbeispiel für die Verwendung der Webauthentifizierungsproxy-Funktion auf einem Wireless LAN Controller (WLC).

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen, bevor Sie diese Konfiguration vornehmen:

- Kenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Sie verfügen über Kenntnisse in den Bereichen LWAPP (Lightweight Access Point Protocol)/CAPWAP (Control and Provisioning of Wireless Access Points).
- Ich habe Kenntnisse in der Webauthentifizierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 4400 WLC mit Firmware-Version 7.0.116.0
- Cisco Serie 1130AG LAP
- Cisco 802.11a/b/g Wireless Client Adapter für Firmware-Version 4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps von Cisco zu Konventionen).

Webauthentifizierungsproxy auf einem WLC

In diesem Dokument wird davon ausgegangen, dass der Leser die Webauthentifizierung und die Schritte zur Konfiguration der Webauthentifizierung auf Cisco WLCs kennt. Wenn Sie ein neuer Benutzer sind, lesen Sie die folgenden Dokumente, in denen der Web-Authentifizierungsprozess im Detail erläutert wird:

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- Problembehandlung bei der Webauthentifizierung auf einem Wireless LAN Controller (WLC)

Die Webauthentifizierungsproxy-Funktion wurde mit WLC Version 7.0.116.0 eingeführt.

Ein Webbrowser verfügt über drei Arten von Interneteinstellungen, die vom Benutzer konfiguriert werden können:

- Automatische Erkennung
- Systemproxy
- Manuell

Mit dieser Funktion können Clients, auf denen ein manueller Webproxy im Browser aktiviert ist, die Webauthentifizierung mit dem Controller vereinfachen.

Wenn der Client in einem für die Webauthentifizierung konfigurierten Netzwerk für manuelle Proxy-Einstellungen konfiguriert ist, hört der Controller diese Proxy-Ports nicht an, sodass der Client keine TCP-Verbindung mit dem Controller herstellen kann. Im Endeffekt kann der Benutzer zu keiner Anmeldeseite gelangen, um sich zu authentifizieren und Zugriff auf das Netzwerk zu erhalten.

Wenn der Client eine URL anfordert, bei der die Webauthentifizierungsproxy-Funktion aktiviert ist, antwortet der Controller mit einer Webseite, auf der der Benutzer aufgefordert wird, die Internet-Proxyeinstellungen zu ändern, um die Proxyeinstellungen automatisch zu erkennen.

Dieser Prozess verhindert, dass die manuellen Proxyeinstellungen des Browsers verloren gehen. Nach der Konfiguration dieser Funktion kann der Benutzer über die Web-Authentifizierungsrichtlinie auf das Netzwerk zugreifen.

Diese Funktion wird standardmäßig für die Ports 80, 8080 und 3128 bereitgestellt, da es sich hierbei um die am häufigsten verwendeten Ports für den Webproxyserver handelt.

Webauthentifizierungsproxy auf einem WLC konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Konfigurationen

Führen Sie die folgenden Schritte aus, um den Webauthentifizierungsproxy über die grafische Benutzeroberfläche des Controllers zu konfigurieren:

- 1. Wählen Sie in der GUI des Controllers **Controller > General (Allgemein)**.
- 2. Um den WebAuth-Proxy zu aktivieren, wählen Sie in der Dropdown-Liste WebAuth Proxy Redirection Mode (WebAuth-Proxyumleitungsmodus) die Option Enabled (Aktiviert) aus.

cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECURITY MANAGEMEN
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 4 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
	WebAuth Proxy Redirection Mode WebAuth Proxy Redirection Port	Enabled Disabled Enabled

3. Geben Sie im Textfeld WebAuth Proxy Redirection Port (WebAuth-Proxy-Umleitungsport) die Portnummer des Web-Authentifizierungsproxys ein. Dieses Textfeld enthält die Portnummern, auf denen der Controller die Weiterleitung des Webauthentifizierungsproxys abhört. Standardmäßig wird von den drei Ports 80, 8080 und 3128 ausgegangen. Wenn Sie den Umleitungsport für die Webauthentifizierung auf einen anderen Port als diese Werte konfiguriert haben, müssen Sie diesen Wert angeben.

uluilu cisco		WIRELESS SECURITY MANAGEMENT COMMANDS HELP	EEEDBACK
Controller	General		
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management	Name 802.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicast Mode J AP Fallback Apple Talk Bri <mark>Microsoft Internet Exp</mark>	WLC-4400 Disabled Disabled Unicast Enabled Unicast Group Address	d). X
Ports NTP CDP	Fast SSID ohe Default Mobili RF Group Nam	n will be enabled for proxy ports 80, 6060 and 3128 by default, and for user-configure the system for the webAuth proxy setting to take effect.	d proxy redirection port if any.
Advanced	User Idle Time 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 Sisabled Commercial (0 to 40 C) 0 to 65 C Enabled 0	

4. Klicken Sie auf Apply (Anwenden).

Führen Sie den folgenden Befehl aus, um den WebAuth-Proxy über die CLI zu konfigurieren:

config network web-auth proxy-redirect {enable | disable} Legen Sie die Webauthentifizierungs-Portnummer mit dem Befehl config network web-auth port <port-number> fest.

Speichern Sie nach der Konfiguration des WLC die Konfiguration, und starten Sie den Controller neu, damit die Konfiguration wirksam wird.

Überprüfung

Um den aktuellen Status der Proxy-Konfiguration für die Webauthentifizierung anzuzeigen, geben Sie entweder den Befehl **show network summary** oder **show running-config ein**.

(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

Verbinden wir nun einen Wireless-Client mit der Gast-SSID, die wir für die Webauthentifizierung konfiguriert haben.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit 'Guest1'
 WLANs WLANs Advanced 	General Security QoS Advanced Profile Name Guest1
	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 Vlan Feature Enabled Broadcast SSID Imagement

Wenn Sie über einen internen DHCP-Server verfügen, stellt der Client eine Verbindung mit dem WLAN Guest1 her und erhält eine IP-Adresse. Wenn der Client versucht, auf eine URL zuzugreifen (z. B. www.cisco.com), da der manuelle Proxy im Client-Browser aktiviert ist, antwortet der Controller, der die Funktion für den Webauthentifizierungsproxy verwendet, mit einer Webseite, die den Benutzer auffordert, die Internet-Proxy-Einstellungen zu ändern, um die Proxy-Einstellungen automatisch zu erkennen.

De Ex Ten utral fromune Tone Bab	
SE X 💿 🛄 http://dsco.com/	
🚵 Most Visited 🥮 Getting Started 🛼 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 Firefox:
	 Go to 'Toola' and select 'Options'. Choose the 'Advanced' settings and click on the 'Network' tab. Click on the 'Settings' button under Connection. Choose 'Auto-detect proxy settings for this setwork' and click OK. Refresh the web page or try another URL.
	Close

An diesem Punkt ist sich der Client bewusst, dass die manuellen Proxy-Einstellungen deaktiviert werden müssen. Hier können Sie sehen, wie Sie die manuellen Proxy-Einstellungen auf Firefox Version 3.6 deaktivieren.

- 1. Wählen Sie im Firefox-Browser **Extras > Optionen** und dann **Erweitert** aus.
- 2. Klicken Sie auf die Registerkarte Netzwerk, und wählen Sie dann Einstellungen

General	Tabs	Content		Privacy	Security	Advanced
General N	etwork	ndate Encr	votion			
Connect	ion re how Fir	efox connec	ts to the Intern	et		Settings
Use up I	to 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	<u>⊂</u> lear Now E <u>x</u> ceptions
						Remove

3. Wählen Sie im Fenster Verbindungseinstellungen die Option **Proxy-Einstellungen für dieses** Netzwerk automatisch erkennen

 Use system prov Manual proxy co 	y settings		
HTTP Proxy:	X.X.X.X	Port:	8080
	Use this proxy se	erver for all protocols	
<u>S</u> SL Proxy:		P <u>o</u> rt:	0
ETP Proxy:		Po <u>r</u> t:	0
<u>G</u> opher Proxy:		Port:	0
SO <u>C</u> KS Host:		Por <u>t</u> :	0
	○ SOCKS v4 ④	SOCKS <u>v</u> 5	
No Proxy for:	localhost, 127.0.0.1		
	Example: .mozilla.org	, .net.nz, 192.168.1.	0/24
	configuration URL:		

.

Aktualisieren Sie anschließend den Browser, und versuchen Sie erneut, auf die URL zuzugreifen. Dieses Mal werden Sie zur Seite für die Webauthentifizierung weitergeleitet. Der Client stellt Ihnen Anmeldeinformationen zur Verfügung, und Sie können sich beim Gastnetzwerk anmelden.

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

Zugehörige Informationen

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- Problembehandlung bei der Webauthentifizierung auf einem Wireless LAN Controller (WLC)
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 7.0.116.0
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.