Configureer de webverificatieproxy op een WLC

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Web verificatie-proxy op een WLC Configureer de webverificatieproxy op een WLC Configuraties Verifiëren Gerelateerde informatie

Inleiding

Dit document biedt een configuratievoorbeeld voor het gebruik van de Web Verification Proxy op een draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Zorg voor kennis van de configuratie van Lichtgewicht access points (LAP's) en Cisco WLC's.
- Heb kennis van Lichtgewicht Access Point Protocol (LWAP)/Control and Provisioning of Wireless Access points (CAPWAP).
- Zorg voor kennis van webverificatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 WLC met firmwarerelease 7.0.116.0
- Cisco 1130AG Series access point
- Cisco 802.11a/b/g draadloze clientadapter waarop firmware-release 4.2 wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Web verificatie-proxy op een WLC

Dit document veronderstelt dat de lezer eerdere kennis heeft van webverificatie en de stappen die betrokken zijn bij het configureren van webverificatie op Cisco WLC's. Als u een nieuwe gebruiker bent, leest u deze documenten waarin u het web-verificatieproces in detail uitlegt:

- Configuratie van draadloze LAN-controller en webverificatie voorbeeld
- <u>Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers</u>
- Webverificatie voor probleemoplossing op een draadloze LAN-controller (WLC)

De webverificatieproxy is geïntroduceerd in WLC versie 7.0.116.0.

Een webbrowser heeft drie soorten internetinstellingen die door de gebruiker kunnen worden geconfigureerd:

- Automatisch detecteren
- Systeemproxy
- Handmatig

Deze eigenschap laat cliënten toe die handwebvolmacht hebben toegelaten in browser om webauthentificatie met het controlemechanisme te vergemakkelijken.

In een netwerk dat is geconfigureerd voor webverificatie, als de client is geconfigureerd voor handmatige proxyinstellingen, luistert de controller niet naar dergelijke proxypoorten en kan de client dus geen TCP-verbinding met de controller tot stand brengen. De gebruiker kan niet naar een inlogpagina voor verificatie en toegang tot het netwerk.

Wanneer de client een URL aanvraagt met de functie Web Verification Proxy ingeschakeld, reageert de controller met een webpagina die de gebruiker vraagt om de proxyinstellingen van het internet te wijzigen om automatisch de proxyinstellingen te detecteren.

Dit proces voorkomt dat de handmatige proxy instellingen van de browser verloren gaan. Na het configureren van deze functie kan de gebruiker toegang krijgen tot het netwerk via het web authenticatiebeleid.

Standaard is deze functionaliteit beschikbaar voor poorten 80, 8080 en 3128, omdat dit de meest gebruikte poorten zijn voor de webproxyserver.

Configureer de webverificatieproxy op een WLC

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Configuraties

Voltooi deze stappen om de Proxy voor webverificatie te configureren met behulp van de controller GUI:

- 1. Kies in de GUI van de controller **Controller** de optie **Controller > Algemeen**.
- 2. Als u WebAuth Proxy wilt inschakelen, kiest u **Ingeschakeld** in de vervolgkeuzelijst **WebAuth Proxy Redirection**

Mode.

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

3. Voer in het tekstvak Webex Proxy Redirection Port het poortnummer van de webverificatieproxy in. Dit tekstvak bestaat uit de poortnummers waarop de controller luistert naar de omleiding van de proxy voor webverificatie. Standaard wordt uitgegaan van de drie poorten 80, 8080 en 3128. Als u de webverificatie-omleidingspoort naar een andere poort dan deze waarden hebt geconfigureerd, moet u die waarde specificeren.

ululu cisco	MONITOR MUANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMMANDS HELP	EEEDBACK
Controller	General			
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP	Name B02.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicest Mode Å AP Fallback Apple Talk Bri Fast SSID che Default Mobili	WLC-4400 Disabled = Disabled = Unicest = 0.0.0.0 Enabled = storrer son will be enabled for procy parts 80 et the system for the webAuth procy	(LAG Mode is currently disabled) Multicast Group Address , 8060 and 3128 by default, and for user-configured) setting to take effect.	Σ proxy redirection port if any.
CDP Advanced	R# Group Nam		CK	
	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 •		

4. Klik op Apply (Toepassen).

Om WebAuth Proxy vanuit de CLI te configureren, geeft u deze opdracht uit:

config network web-auth proxy-redirect {enable | disable} Stel het poortnummer voor webverificatie in met de opdracht web-auth poort voor *<poortnummer>* voor configuratie.

Zodra de WLC is geconfigureerd, slaat u de configuratie op en start u de controller opnieuw op, zodat de configuratie van kracht kan worden.

Verifiëren

Om de huidige status van de configuratie van de de volmacht van de webauthentificatie te zien, geef of de samenvatting van het shownetwerk uit of toon in werking stelt -in werking stellenconfiguratiebevel.

(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

Laten we nu een draadloze client verbinden met de Guest SSID die we hebben geconfigureerd voor webverificatie.

cisco	Monitor wlans controller wireless security management commands help f
WLANs	WLANs > Edit 'Guest1'
 WLANs WLANs Advanced 	General Security QoS Advanced Profile Name GuestI Type WLAN SSID GuestI Status Image: 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

Aangenomen dat u een interne DHCP-server heeft, sluit de client zich aan op de WLAN Guest1 en krijgt een IP-adres. Wanneer de client probeert toegang te krijgen tot een URL (bijvoorbeeld www.cisco.com), aangezien handproxy is ingeschakeld op de clientbrowser, reageert de controller met de webverificatie-proxyfunctie met een webpagina die de gebruiker vraagt om de instellingen van de internetproxy te wijzigen om automatisch de proxyinstellingen te detecteren.



Op dit punt is de client zich ervan bewust dat de handmatige proxy instellingen moeten worden uitgeschakeld. Hier kun je zien hoe je de handmatige proxy-instellingen uitschakelt op Firefox versie 3.6.

- 1. Selecteer vanuit de Firefox-browser **Gereedschappen > Opties** en selecteer vervolgens **Geavanceerd**.
- 2. Klik op het tabblad **Netwerk** en selecteer **Instellingen**.

	X
General Tabs Content Applications Privacy Security Advanced	
General Network Update Encryption	
Configure how Firefox connects to the Internet	
Offline Storage Use up to 50 Image Image: Tell me when a web site asks to store data for offline use The following web sites have stored data for offline use:	
Remove	

3. Selecteer in het venster Verbindingsinstellingen de optie Proxy-instellingen automatisch detecteren voor dit

Use system prov Manual proxy co	y settings	
HTTP Proxy:	X.X.X.X Port:	8080
	Use this proxy server for all protocols	
<u>S</u> SL Proxy:	Port:	0
ETP Proxy:	Port:	0
<u>G</u> opher Proxy:	Port:	0
SO <u>C</u> KS Host:	Por <u>t</u> :	0
	○ SOCKS v4 ③ SOCKS v5	
No Proxy for:	localhost, 127.0.0.1	
	Example: .mozilla.org, .net.nz, 192.168.1	0/24

netwerk.

Vernieuw de browser en probeer de URL opnieuw te openen als dit is voltooid. Ditmaal wordt u doorgestuurd naar de pagina Web Verification. De client kan u van referenties voorzien en u kunt inloggen op het gastennetwerk.

Web Authentication	÷	
Login		

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

Gerelateerde informatie

- <u>Configuratie van draadloze LAN-controller en webverificatie voorbeeld</u>
- <u>Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers</u>
- Webverificatie voor probleemoplossing op een draadloze LAN-controller (WLC)
- <u>Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.