WLC(Wireless LAN Controller)에 대한 웹 인증 이해

목차

소개

이 문서에서는 WLC(Wireless LAN Controller)의 웹 인증 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

WLC 컨피그레이션에 대한 기본 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 모든 WLC 하드웨어 모델을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

웹 인증 내부 프로세스

보안 기능으로서의 웹 인증 위치

웹 인증(WebAuth)은 레이어 3 보안입니다. 브라우저를 실행하는 모든 스테이션에서 작동하는 사용자 친화적인 보안을 허용합니다.

사전 공유 키(PSK) 보안(레이어 2 보안 정책)과 결합할 수 있습니다.

WebAuth와 PSK의 조합으로 사용자에게 친숙한 부분이 줄어들지만 클라이언트 트래픽을 암호화할 수 있는 이점이 있습니다.

WebAuth는 암호화 없는 인증 방법입니다.

WLC 소프트웨어 릴리스 7.4를 설치하고 동시에 구성해야 802.1x/RADIUS(Remote Authentication Dial-In User Service)로 WebAuth를 구성할 수 있습니다.

클라이언트는 dot1x 및 웹 인증을 모두 거쳐야 합니다. 게스트가 아닌 직원(802.1x 사용)을 위한 웹 포털을 추가하기 위한 것입니다.

직원용 dot1x 또는 게스트용 웹 포털에 대한 올인원 SSID(Service Set Identifier)가 없습니다.

WebAuth 작동 방식

802.11 인증 프로세스가 열려 있으므로 아무 문제 없이 인증하고 연결할 수 있습니다. 그 이후에는 WLC에 연결되지 않지만 **RUN** 상태.

웹 인증이 활성화되면 **WEBAUTH_REQD** 네트워크 리소스에 액세스할 수 없는 경우

옵션에서 DNS 서버 주소와 함께 DHCP IP 주소를 수신해야 합니다.

브라우저에 유효한 URL을 입력합니다. 클라이언트는 DNS 프로토콜을 통해 URL을 확인합니다. 클라이언트는 웹 사이트의 IP 주소로 HTTP 요청을 보냅니다.

WLC가 해당 요청을 인터셉트하고 **webauth** 로그인 페이지 - 웹 사이트 IP 주소를 모방합니다. 외부 WebAuth를 사용하면 WLC가 웹 사이트 IP 주소 및 페이지가 이동했다는 상태를 포함하는 HTTP 응답으로 응답합니다.

페이지가 WLC에서 사용하는 외부 웹 서버로 이동되었습니다. 인증을 받으면 모든 네트워크 리소스에 액세스할 수 있으며 기본적으로 원래 요청된 URL로 리디렉션됩니다(WLC에서 강제 리디렉션이 구성되지 않은 경우).

요약하면, WLC는 클라이언트가 DNS를 확인하고 IP 주소를 자동으로 **WEBAUTH_REQD** 상태.

포트 80 대신 다른 포트를 보려면 **config network web-auth-port** 이 포트에서 리디렉션을 생성합니다.

예를 들어 ACS(Access Control Server) 웹 인터페이스가 포트 2002 또는 기타 유사한 애플리케이션에 있습니다.

> **HTTPS 리디렉션에 대한 참고 사항**: 기본적으로 WLC는 HTTPS 트래픽을 리디렉션하지 않았습니다. 즉, 브라우저에 HTTPS 주소를 입력하면 아무 일도 일어나지 않습니다. HTTPS에서 제공된 로그인 페이지로 리디렉션하려면 HTTP 주소를 입력해야 합니다.
>
> 버전 8.0 이상에서는 CLI 명령을 사용하여 HTTPS 트래픽의 리디렉션을 활성화할 수 있습니다 **config network web-auth https-redirect enable.**
>
> 많은 HTTPS 요청이 전송되는 경우 WLC에 많은 리소스를 사용합니다. 이 기능의 확장성이 향상된 WLC 버전 8.7 전에는 이 기능을 사용하지 않는 것이 좋습니다. 또한 이 경우에는 인증서 경고가 불가피하다는 점에 유의하십시오. 클라이언트가 URL(예: https://www.cisco.com)을 요청하더라도 WLC는 가상 인터페이스 IP 주소에 대해 발급된 자체 인증서를 계속 제공합니다. 이는 클라이언트가 요청한 URL/IP 주소와 일치하지 않으며, 클라이언트가 브라우저에 예외를 적용하지 않는 한 인증서를 신뢰할 수 없습니다.

8.7 측정 전 WLC 소프트웨어 릴리스의 성능 저하를 나타냅니다.

웹 인증	**달성률**
URL 3개 - HTTP	140/초
첫 번째 URL - HTTP 두 번째 및 세 번째 URL - HTTPS	20/초
URL 3개 - HTTPS(대규모 구축)	<1/초
URL 3개 - HTTPS(최대 100개 클라이언트)	10/초

이 성능 테이블에서 3개의 URL은 다음과 같습니다.

- 최종 사용자가 입력한 원래 URL
- WLC가 브라우저를 리디렉션하는 URL
- 최종 자격 증명 제출

성능 테이블은 3개의 URL이 모두 HTTP인 경우, 3개의 URL이 모두 HTTPS인 경우 또는 클라이언트가 HTTP에서 HTTPS(일반)로 이동하는 경우 WLC 성능을 제공합니다.

내부(로컬) WebAuth가 내부 페이지에서 작동하도록 하는 방법

운영 동적 인터페이스로 WLAN을 구성하려면 클라이언트도 DHCP를 통해 DNS 서버 IP 주소를 수신합니다.

항상 **webauth** 를 설정하고 WLAN이 제대로 작동하는지, DNS 요청을 확인할 수 있는지 확인합니다(**nslookup**)와 웹 페이지를 탐색할 수 있습니다.

웹 인증을 Layer 3 보안 기능으로 설정합니다. 로컬 데이터베이스 또는 외부 RADIUS 서버에서 사용자를 생성합니다.

무선 LAN 컨트롤러 웹 인증 컨피그레이션 예시 문서를 참조하십시오.

사용자 지정 페이지를 사용하여 사용자 지정 로컬 WebAuth를 구성하는 방법

사용자 지정 **webauth** 구성 가능 **redirectUrl** 에서 **Security** 탭. 이렇게 하면 사용자가 입력하는 특정 웹 페이지로 리디렉션됩니다.

사용자가 인증되면 클라이언트가 요청한 원래 URL을 재정의하고 리디렉션이 할당된 페이지를 표시합니다.

사용자 지정 기능을 사용하면 기본 로그인 페이지 대신 사용자 지정 HTML 페이지를 사용할 수 있습니다. html 및 이미지 파일 번들을 컨트롤러에 업로드합니다.

업로드 페이지에서 **webauth bundle** tar 형식 PicoZip은 WLC와 호환되는 tar를 생성합니다.

WebAuth 번들의 예는 무선 컨트롤러 WebAuth 번들에 대한 소프트웨어 다운로드 페이지를 참조하십시오. WLC에 적합한 릴리스를 선택합니다.

존재하는 번들을 사용자 정의하는 것이 좋습니다. 새 번들을 생성하지 마십시오.

다음과 같은 몇 가지 제한 사항이 있습니다 **custom webauth** 버전 및 버그에 따라 다릅니다.

- .tar 파일 크기(5MB 이하)
- .tar의 파일 수
- 파일의 파일 이름 길이(최대 30자)

패키지가 작동하지 않으면 간단한 사용자 지정 패키지를 시도합니다. 사용자가 사용하려는 패키지에 도달하기 위해 개별적으로 파일 및 복잡성을 추가합니다. 그러면 문제를 파악하는 데 도움이 됩니다.

사용자 지정 페이지를 구성하려면 Cisco Wireless LAN Controller Configuration Guide, Release 7.6의 섹션에서 Creating a Customized Web Authentication Login Page를 참조하십시오.

전역 구성 기술 재정의

override global config **명령을** 사용하여 구성하고 각 WLAN에 대한 WebAuth 유형을 설정합니다. 이렇게 하면 다른 WLAN에 대해 맞춤형 내부/기본 WebAuth를 사용하는 내부/기본 WebAuth가 허용됩니다.

이렇게 하면 각 WLAN에 대해 서로 다른 사용자 지정 페이지를 구성할 수 있습니다.

동일한 번들의 모든 페이지를 결합하여 WLC에 업로드합니다.

각 WLAN에서 override **global config 명령**으로 사용자 지정 페이지를 설정하고 번들에 있는 모든 파일에서 어떤 파일이 로그인 페이지인지 선택합니다.

각 WLAN에 대한 번들 내의 다른 로그인 페이지를 선택합니다.

리디렉션 문제

HTML 번들 내에는 리디렉션을 허용하는 변수가 있습니다. 강제 리디렉션 URL을 입력하지 마십시오.

사용자 지정 WebAuth에서 리디렉션 문제가 발생할 경우 번들을 확인하는 것이 좋습니다.

WLC GUI에 **+=로** 리디렉션 URL을 입력하면 번들 내에 정의된 URL을 덮어쓰거나 추가할 수 *있습니다*.

예를 들어, WLC GUI에서 **redirectURL** 필드가 www.cisco.com으로 설정됩니다. 그러나 번들에는 다음이 표시됩니다. **redirectURL+=** '(웹 사이트 URL)'. **+=**는 사용자를 잘못된 URL로 리디렉션합니다.

외부(로컬) 웹 인증이 외부 페이지에서 작동하도록 하는 방법

외부 WebAuth 서버의 활용은 로그인 페이지의 외부 저장소일 뿐입니다. 사용자 자격 증명은 WLC에서 계속 인증됩니다. 외부 웹 서버는 특수 또는 다른 로그인 페이지만 허용합니다.

외부 WebAuth에 대해 수행되는 단계:

1. 클라이언트(최종 사용자)가 웹 브라우저를 열고 URL을 입력합니다.

2. 클라이언트가 인증되지 않고 외부 웹 인증이 사용되는 경우 WLC는 사용자를 외부 웹 서버 URL로 리디렉션합니다. WLC는 HTTP 리디렉션을 모방된 IP 주소로 클라이언트에 전송하고 외부 서버 IP 주소를 가리킵니다. 외부 웹 인증 로그인 URL에는 **AP_Mac_Address,**이 **client_url** (**클라이언트 URL 주소**) 및 **action_URL** 스위치 웹 서버에 연결해야 합니다.

3. 외부 웹 서버 URL은 사용자를 로그인 페이지로 전송합니다. 사용자는 사전 인증 ACL(access control list)을 사용하여 서버에 액세스할 수 있습니다.

4. 로그인 페이지에서 사용자 자격 증명 요청을 로 다시 보냅니다. **action_URL**WLC 웹 서버의 http://192.0.2.1/login.html과 같은 이는 리디렉션 URL에 대한 입력 매개변수로 제공됩니다. 여기서 192.0.2.1은 스위치의 가상 인터페이스 주소입니다.

5. WLC 웹 서버는 인증을 위해 사용자 이름 및 비밀번호를 제출합니다.

6. WLC는 RADIUS 서버 요청을 시작하거나 WLC의 로컬 데이터베이스를 사용한 다음 사용자를 인증합니다.

7. 인증에 성공하면 WLC 웹 서버는 구성된 리디렉션 URL 또는 클라이언트가 입력한 URL로 사용자를 전달합니다.

8. 인증이 실패하면 WLC 웹 서버는 사용자를 사용자 로그인 URL로 다시 리디렉션합니다.

   참고: 이 문서에서는 가상 ip의 예로 192.0.2.1을 사용합니다. 192.0.2.x 범위는 라우팅할 수 없으므로 가상 ip에 사용하는 것이 좋습니다. 이전 설명서는 "1.1.1.x"를 참조하거나 기본 설정이었던 것처럼 여전히 WLC에 구성되어 있습니다. 그러나 이 ip는 이제 유효한 라우팅 가능한 ip 주소이므로 192.0.2.x 서브넷이 권장됩니다.

액세스 포인트(AP)가 FlexConnect 모드인 경우 **preauth** ACL은 관련이 없습니다. Flex ACL을 사용하여 인증되지 않은 클라이언트의 웹 서버에 대한 액세스를 허용할 수 있습니다.

무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예를 참조하십시오.

웹 통과

웹 통과는 내부 웹 인증의 변형입니다. 경고 또는 경고 문이 있는 페이지를 표시하지만 자격 증명을 묻는 메시지를 표시하지 않습니다.

그런 다음 사용자는 ok(**확인**)를 **클릭합니다**. 이메일 입력을 활성화하면 사용자는 자신의 사용자 이름이 되는 이메일 주소를 입력할 수 있습니다.

사용자가 연결되면 활성 클라이언트 목록을 확인하고 사용자가 사용자 이름으로 입력한 이메일 주소와 함께 나열되는지 확인합니다.

자세한 내용은 Wireless LAN Controller 5760/3850 Web Passthrough 컨피그레이션 예를 참조하십시오.

조건부 웹 리디렉션

조건부 웹 리디렉션을 활성화하면 802.1x 인증이 성공적으로 완료된 후 사용자가 특정 웹 페이지로 조건부 리디렉션됩니다.

RADIUS 서버에서 리디렉션이 발생하는 조건 및 리디렉션 페이지를 지정할 수 있습니다.

만료일에 도달하거나 사용자가 계속 사용/액세스하기 위해 청구서를 지불해야 하는 경우 조건에 비밀번호가 포함될 수 있습니다.

RADIUS 서버가 Cisco AV 쌍을 반환 하는 경우 **url-redirect**그러면 사용자가 브라우저를 열 때 지정된 URL로 리디렉션됩니다.

서버가 Cisco AV-pair도 반환하는 경우 **url-redirect-acl**지정된 ACL이 이 클라이언트에 대한 사전 인증 ACL로 설치됩니다.

이 시점에서 클라이언트는 완전히 인증된 것으로 간주되지 않으며 사전 인증 ACL에서 허용하는 트래픽만 전달할 수 있습니다. 클라이언트가 지정된 URL에서 특정 작업(예: 비밀번호 변경 또는 청구 결제)을 완료한 후 클라이언트를 다시 인증해야 합니다.

RADIUS 서버가 다음을 반환하지 않는 경우 **url-redirect**에서는 클라이언트가 완전히 인증된 것으로 간주되며 트래픽을 전달할 수 있습니다.

> **참고:** 조건부 웹 리디렉션 기능은 802.1x 또는 WPA+WPA2 레이어 2 보안을 위해 구성된 WLAN에만 사용할 수 있습니다.

RADIUS 서버를 구성한 후 컨트롤러 GUI 또는 CLI를 사용하여 컨트롤러에서 조건부 웹 리디렉션을 구성합니다. 다음 단계별 가이드를 참조하십시오. 웹 리디렉션 구성(GUI) 및 웹 리디렉션 구성(CLI).

스플래시 페이지 웹 리디렉션

스플래시 페이지 웹 리디렉션을 활성화하면 802.1x 인증이 성공적으로 완료된 후 사용자가 특정 웹 페이지로 리디렉션됩니다. 리디렉션 후에는 사용자가 네트워크에 대한 전체 액세스 권한을 갖습니다.

RADIUS 서버에서 리디렉션 페이지를 지정할 수 있습니다. RADIUS 서버가 Cisco AV 쌍을 반환 하는 경우 **url-redirect**그러면 사용자가 브라우저를 열 때 지정된 URL로 리디렉션됩니다.

이 시점에서 클라이언트는 완전히 승인된 것으로 간주되며 RADIUS 서버가 트래픽을 반환하지 않더라도 트래픽을 전달할 수 있습니다 **url-redirect.**

> **참고:** 스플래시 페이지 리디렉션 기능은 802.1x 또는 WPA+WPA2 레이어 2 보안을 위해 구성된 WLAN에만 사용할 수 있습니다.

RADIUS 서버를 구성한 후 컨트롤러 GUI 또는 CLI를 사용하여 컨트롤러의 스플래시 페이지 웹 리디렉션을 구성합니다.

MAC에서 웹 인증 필터 실패

MAC 필터 FaFailure의 WebAuth를 사용하려면 Layer 2 보안 메뉴에서 MAC 필터를 구성해야 합니다.

사용자가 MAC 주소로 성공적으로 검증되면 **run** 상태.

그렇지 않으면 **WEBAUTH_REQD** 상태 및 일반 웹 인증이 발생합니다.

> **참고:** 웹 패스스루에서는 지원되지 않습니다.자세한 내용은 개선 요청 Cisco 버그 ID CSCtw의 활동을 참조하십시오73512

중앙 웹 인증

중앙 웹 인증은 WLC가 더 이상 서비스를 호스팅하지 않는 시나리오를 의미합니다. 클라이언트는 ISE 웹 포털로 직접 전송되며 WLC에서 192.0.2.1을 거치지 않습니다. 로그인 페이지 및 전체 포털이 외부화됩니다.

WLAN 및 MAC 필터의 고급 설정에서 RADIUS NAC(Network Admission Control)를 활성화하면 중앙 웹 인증이 수행됩니다.

WLC는 RADIUS 인증(일반적으로 MAC 필터용)을 ISE에 전송하며, ISE는 **redirect-url** AV(특성 값) 쌍

그러면 사용자가 **POSTURE_REQD** ISE가 CoA(Change of Authorization) 요청을 통해 권한을 부여할 때까지 상태를 지정합니다. 포스처 또는 중앙 WebAuth에서도 동일한 시나리오가 발생합니다.

게스트 포털이 EAP(Extensible Authentication Protocol)와 마찬가지로 암호화를 위한 세션 키를 반환할 수 없기 때문에 중앙 WebAuth는 WPA-엔터프라이즈/802.1x와 호환되지 않습니다.

외부 사용자 인증(RADIUS)

RADIUS(External User Authentication)는 WLC에서 자격 증명을 처리하거나 레이어 3 웹 정책이 활성화된 경우에만 로컬 웹 인증에 유효합니다. RADIUS를 통해 로컬에서 또는 WLC에서 또는 외부에서 사용자를 인증합니다.

WLC가 사용자의 자격 증명을 확인하는 순서가 있습니다.

1. 어떤 경우든 먼저 자체 데이터베이스에서 검색합니다.
2. 사용자가 없는 경우 게스트 WLAN에 구성된 RADIUS 서버로 이동합니다(구성된 사용자가 있는 경우).
3. 그런 다음 RADIUS 서버에 대해 전역 RADIUS 서버 목록을 확인합니다. **network user** 을(를) 선택합니다.

이 세 번째 포인트는 해당 WLAN에 대해 RADIUS를 구성하지 않는 사용자의 질문에 대한 답변이지만, 사용자가 컨트롤러에서 발견되지 않을 때에도 RADIUS를 확인합니다.

이는 **network user** 전역 목록에서 RADIUS 서버에 대해 확인됩니다.

WLC는 PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol) 또는 EAP-MD5(Message Digest5)를 사용하여 RADIUS 서버에 사용자를 인증할 수 있습니다.

전역 매개변수이며 GUI 또는 CLI에서 구성할 수 있습니다.

GUI에서: 탐색 **Controller > Web RADIUS Authentication**

CLI에서: 입력 사항 **config custom-web RADIUSauth**

참고:NAC 게스트 서버는 PAP만 사용합니다.

유선 게스트 WLAN 설정 방법

유선 게스트 WLAN 컨피그레이션은 무선 게스트 컨피그레이션과 유사합니다. 하나 또는 두 개의 컨트롤러로 구성할 수 있습니다(하나의 컨트롤러가 자동 앵커인 경우에만).

유선 게스트 사용자의 VLAN으로 VLAN을 선택합니다(예: VLAN 50). 유선 게스트가 인터넷에 액세스하려는 경우 VLAN 50에 대해 구성된 스위치의 포트에 랩톱을 연결합니다.

이 VLAN 50은 허용되어야 하며 WLC 트렁크 포트를 통해 경로에 있어야 합니다.

WLC가 2개인 경우(앵커 1개와 외부 1개), 이 유선 게스트 VLAN은 외부 WLC(WLC1)로 연결해야 하며 앵커로 연결해서는 안 됩니다.

그런 다음 WLC1은 DMZ WLC(앵커, WLC2)에 대한 트래픽 터널을 관리하며, 이는 라우팅된 네트워크의 트래픽을 릴리스합니다.

유선 게스트 액세스를 구성하는 5단계는 다음과 같습니다.

1. **유선 게스트 사용자 액세스를 위한 동적 인터페이스(VLAN)를 구성합니다.**

   WLC1에서 동적 인터페이스 VLAN50을 생성합니다. **interface configuration** 페이지에서 **Guest LAN** 상자를 클릭합니다. 그런 다음 **IP address** 및 **gateway** 사라져 WLC는 트래픽이 VLAN 50에서 라우팅됨을 인식해야 합니다. 이러한 클라이언트는 유선 게스트입니다.

2. **게스트 사용자 액세스를 위한 유선 LAN을 생성합니다.**

   컨트롤러에서 인터페이스는 WLAN에 연결될 때 사용됩니다. 그런 다음 본사 컨트롤러에

WLAN을 생성합니다. 탐색 **WLANs** 및 **New**. 수신 **WLAN Type**, 선택 **Guest LAN**.

Profile **Name** and **WLAN SSID**(**프로파일 이름** 및 WLAN SSID)에 이 WLAN을 식별하는 이름을 입력합니다. 이 이름은 다를 수 있지만 공백을 포함할 수 없습니다. WLAN이라는 용어가 사용되지만 이 네트워크 프로파일은 무선 네트워크 프로파일과 관련이 없습니다.

이 **General** 이 탭은 두 개의 드롭다운 목록을 제공합니다. **Ingress** 및 **Egress**. 인그레스(ingress)는 사용자가 들어오는 VLAN입니다(VLAN 50). 이그레스(egress)는 패킷을 전송하는 VLAN입니다.

대상 **Ingress**, 선택 **VLAN50**.

대상 **Egress**하지만 다릅니다. 컨트롤러가 하나뿐인 경우 다른 동적 인터페이스인 **standard** (게스트 LAN이 아닌) 한 번만 클릭하면 유선 사용자를 이 인터페이스로 보냅니다. 이 경우 DMZ 컨트롤러로 보냅니다. 따라서 **Egress** 인터페이스에서 **Management Interface**.

이 **Security** 이 게스트 LAN "WLAN"의 모드는 WebAuth이며, 이는 허용됩니다. 클릭 **Ok** 확인할 수 있습니다.

3. **외부 컨트롤러(본사)를 구성합니다.**

에서 **WLAN list**, 클릭 **Mobility Anchor** 의 끝에 **Guest LAN** DMZ 컨트롤러를 선택합니다. 여기서는 두 컨트롤러가 서로 인식한다고 가정합니다. 그렇지 않으면 **Controller** > **Mobility Management** > **Mobility group**WLC1에 **DMZWLC**를 추가한 다음 DMZ에 **WLC1**을 추가합니다. 두 컨트롤러가 동일한 모빌리티 그룹에 있어서는 안 됩니다. 그렇지 않으면 기본 보안 규칙이 위반됩니다.

4. **앵커 컨트롤러(DMZ 컨트롤러)를 구성합니다.**

본사 컨트롤러가 준비되었습니다. 이제 DMZ 컨트롤러를 준비합니다. DMZ 컨트롤러에 대한 웹 브라우저 세션을 열고 WLAN으로 **이동합니다**. 새 WLAN을 생성합니다. 수신 **WLAN Type**, 선택 **Guest LAN**.

수신 **Profile Name** 및 **WLAN SSID**, 이 WLAN을 식별하는 이름을 입력합니다. 본사 컨트롤러에 입력한 것과 동일한 값을 사용합니다.

이 **Ingress** 인터페이스가 **None**. 트래픽은 EoIP(Ethernet over IP) 터널을 통해 수신되므로 상관없습니다. 인그레스 인터페이스를 지정할 필요가 없습니다.

이 **Egress** 인터페이스가 클라이언트를 전송할 위치입니다. 예를 들어 **DMZ VLAN** VLAN 9입니다. DMZWLC에서 VLAN 9에 대한 표준 동적 인터페이스를 생성한 다음 **VLAN 9** 액세스 권한을 부여합니다.

Mobility Anchor 터널의 끝을 구성합니다. **WLAN** 목록에서 을 선택합니다 **Mobility Anchor for Guest LAN**. 트래픽을 로컬 컨트롤러인 DMZWLC로 **전송합니다**. 이제 양끝이 모두 준비되었습니다.

5. **게스트 LAN을 미세 조정합니다.**

양쪽 끝에서 WLAN 설정을 세부적으로 조정할 수도 있습니다. 설정은 양쪽 끝에서 동일해야 합니다. 예를 들어 **WLAN Advanced** 탭, **Allow AAA override** wlc1의 경우 DMZWLC에서 동일한 확인란을 선택합니다. 양쪽 WLAN에 차이가 있으면 터널이 중단됩니다. DMZWLC가 트래픽을 거부합니다. Cisco에서 제공하는 **run debug mobility.**

모든 값은 실제로 DMZWLC에서 얻는다는 점에 유의하십시오. IP 주소, VLAN 값 등 WLC1 측을 동일하게 구성하여 WLCDMZ에 요청을 릴레이합니다.

로그인 페이지용 인증서

이 섹션에서는 WebAuth 페이지에 자체 인증서를 배치하거나 192.0.2.1 WebAuth URL을 숨기고 명명된 URL을 표시하는 프로세스를 제공합니다.

컨트롤러 웹 인증용 인증서 업로드

GUI(**WebAuth > Certificate**) 또는 CLI(전송 유형) **webauthcert**)에서 인증서를 업로드할 수 있습니다.

CA(Certificate Authority)로 만든 인증서든 타사 공식 인증서든 상관없이 .pem 형식이어야 합니다.

보내기 전에 인증서의 키도 입력해야 합니다.

업로드 후 인증서를 사용하려면 재부팅해야 합니다. 재부팅되면 GUI의 WebAuth certificate 페이지로 이동하여 업로드한 인증서의 세부사항(유효성 등)을 찾습니다.

중요 한 필드는 일반 적 인 이름 (CN), 인증서에 발급 된 이름 입니다. 이 필드는 이 문서에서 "Certificate Authority and Other Certificates on the Controller(컨트롤러의 인증 기관 및 기타 인증서)" 섹션에 설명되어 있습니다.

재부팅하고 인증서의 세부사항을 확인하면 WebAuth 로그인 페이지에 새 컨트롤러 인증서가 표시됩니다. 하지만 두 가지 상황이 있을 수 있습니다.

1. 모든 컴퓨터가 신뢰하는 몇 가지 기본 루트 CA 중 하나에서 인증서를 발급한 경우에는 괜찮습니다. 예를 들어 VeriSign이 있지만 일반적으로 루트 CA가 아닌 Verisign 하위 CA에 의해 서명됩니다. 신뢰할 수 있는 것으로 언급된 CA가 표시되는 경우 브라우저 인증서 저장소에서 확인할 수 있습니다.

2. 소규모 회사/CA에서 인증서를 받은 경우 모든 컴퓨터가 인증서를 신뢰하지 않습니다. 클라이언트에 회사/CA 인증서를 제공하면 루트 CA 중 하나가 해당 인증서를 발급합니다. 결국 "Certificate have been issued by CA x > CA x certificate has issued by CA y > CA y certificate has issued by this trusted root CA"와 같은 체인이 있습니다. 최종 목표는 클라이언트가 신뢰하는 CA에 도달하는 것입니다.

컨트롤러의 인증 기관 및 기타 인증서

"이 인증서를 신뢰할 수 없습니다."라는 경고를 제거하려면 컨트롤러에서 컨트롤러 인증서를 발급한 CA의 인증서를 입력하십시오.

그런 다음 컨트롤러는 두 인증서(컨트롤러 인증서 및 CA 인증서)를 모두 제공합니다. CA 인증서는 신뢰할 수 있는 CA이거나 CA를 확인할 수 있는 리소스가 있어야 합니다. 실제로 신뢰할 수 있는

CA를 맨 위로 유도하는 CA 인증서 체인을 작성할 수 있습니다.

전체 체인을 같은 파일에 배치합니다. 그러면 파일에는 다음 예와 같은 내용이 포함됩니다.

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

인증서가 URL과 일치하도록 하는 방법

자신을 인증하고 인증서가 발급되기 위해 WebAuth URL은 192.0.2.1로 설정됩니다(WLC 인증서의 CN 필드).

예를 들어 WebAuth URL을 'myWLC.com'으로 변경하려면 **virtual interface configuration** (192.0.2.1 인터페이스) 여기서 **virtual DNS hostname**예: myWLC.com.

이렇게 하면 URL 표시줄의 192.0.2.1이 대체됩니다. 이 이름도 확인 가능해야 합니다. 스니퍼 추적은 모두 작동하는 방식을 보여주지만, WLC가 로그인 페이지를 보낼 때 WLC는 myWLC.com 주소를 보여주고 클라이언트는 이 이름을 DNS로 확인합니다.

이 이름은 192.0.2.1로 확인해야 합니다. 즉, WLC 관리에 이름을 사용하는 경우 WebAuth에 다른 이름을 사용합니다.

WLC 관리 IP 주소에 매핑된 myWLC.com을 사용하는 경우 myWLCwebauth.com과 같은 다른 WebAuth 이름을 사용해야 합니다.

인증서 문제 해결

이 섹션에서는 인증서 문제를 해결하기 위해 확인하는 방법과 내용에 대해 설명합니다.

확인 방법

OpenSSL(Windows의 경우, OpenSSL Win32 검색)을 다운로드하고 설치합니다. 컨피그레이션이 없으면 bin 디렉토리로 이동하여 **openssl s_client –connect (your web auth URL):443**,

이 URL이 WebAuth 페이지가 DNS에 연결된 URL인 경우 이 문서의 다음 섹션에서 "확인 사항"을 참조하십시오.

인증서가 사설 CA를 사용하는 경우 루트 CA 인증서를 로컬 시스템의 디렉토리에 두고 openssl 옵션을 사용합니다 **-CApath**. 중간 CA가 있는 경우 동일한 디렉토리에도 배치합니다.

인증서에 대한 일반 정보를 얻고 확인하려면 다음을 사용합니다.

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

또한 openssl을 사용하여 인증서를 변환하는 것도 유용합니다.

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

확인 사항

클라이언트가 연결될 때 어떤 인증서가 클라이언트에 전송되는지 확인할 수 있습니다. 디바이스 인증서 읽기 — CN은 웹 페이지에 접근할 수 있는 URL이어야 합니다.

디바이스 인증서의 "발급자" 행을 읽습니다. 두 번째 인증서의 CN과 일치해야 합니다. 이 두 번째 인증서인 "issued by"는 다음 인증서의 CN과 일치해야 합니다. 그렇지 않으면, 그것은 진짜 체인을 만들지 않는다.

여기에 표시된 OpenSSL 출력에서 **openssl** "issued by(발급자)"가 제공된 CA 인증서의 이름과 일치하지 않으므로 디바이스 인증서를 확인할 수 없습니다.

SSL 출력

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

또 다른 가능한 문제는 인증서를 컨트롤러에 업로드할 수 없다는 것입니다. 이러한 상황에서는 CA, CA 등의 타당성의 문제가 없습니다.

이를 확인하려면 TFTP(Trivial File Transfer Protocol) 연결을 확인하고 컨피그레이션 파일을 전송해 보십시오. 를 입력하면 **debug transfer all enable** 명령에서 문제는 인증서를 설치하는 것입니다.

인증서에 사용된 키가 잘못되었기 때문일 수 있습니다. 또한 인증서가 잘못된 형식이거나 손상되었을 수 있습니다.

Cisco에서는 인증서 내용을 알려진 유효한 인증서와 비교하는 것을 권장합니다. 이렇게 하면 **LocalkeyID** 특성이 모든 0을 표시합니다(이미 발생함). 그럴 경우 인증서를 다시 변환해야 합니다.

OpenSSL에는 .pem에서 .p12로 반환한 다음 원하는 키로 .pem을 재실행할 수 있는 두 가지 명령이 있습니다.

인증서 뒤에 키가 포함된 .pem을 받은 경우 키 부분을 복사/붙여넣습니다. **----BEGIN KEY ---- until ------- END KEY ------** .pem에서 "key.pem"으로 변경됩니다.

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? 키를 입력하라는 메시지가 표시됩니다. 입력 사항 **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** 이렇게 하면 .pem이 비밀번호로 작동합니다 **check123**.

기타 문제 해결

이 **문서**에서 모빌리티 앵커에 대해 설명하지는 않았지만, **고정된 게스트** 상황인 경우 모빌리티 교환이 올바르게 수행되는지 그리고 클라이언트가 앵커에 도착하는지 확인합니다.

추가 WebAuth 문제는 앵커에서 트러블슈팅을 해야 합니다.

다음은 트러블슈팅할 수 있는 몇 가지 일반적인 문제입니다.

- **사용자는 게스트 WLAN에 연결할 수 없습니다**.

  이는 WebAuth와 관련이 없습니다. 클라이언트 컨피그레이션, WLAN의 보안 설정(활성화된 경우), 무선 장치의 활성 및 작동 여부 등을 확인합니다.

- **사용자가 IP 주소를 가져오지 않습니다**.

  게스트 앵커 상황에서는 외관과 앵커가 정확히 같은 방식으로 구성되지 않았기 때문에 이 경우가 가장 많습니다. 그렇지 않으면 DHCP 컨피그레이션, 연결 등을 확인합니다.
- 다른 WLAN이 문제 없이 동일한 DHCP 서버를 사용할 수 있는지 확인합니다. 이것은 여전히 WebAuth와 관련 되지 않습니다.

- **사용자가 로그인 페이지로 리디렉션되지 않습니다**.

  가장 흔한 증상이지만 더 정확합니다. 두 가지 시나리오가 있습니다.

  사용자가 리디렉션되지 않습니다(사용자가 URL을 입력하고 WebAuth 페이지에 도달하지 않음). 이 경우 다음을 확인하십시오.

  유효한 DNS 서버가 DHCP를 통해 클라이언트에 할당되었는지 여부(**ipconfig /all**),

  클라이언트에서 DNS에 연결할 수 있습니다(**nslookup (website URL**),

사용자가 리디렉션하기 위해 유효한 URL을 입력했음을 나타냅니다.

사용자가 포트 80에서 HTTP URL로 이동했음을 나타냅니다(예: http://localhost:2002을 사용하여 ACS에 연결하기 위해 포트 2002에서 80 대신 전송했으므로 리디렉션하지 않음).

사용자가 192.0.2.1로 올바르게 리디렉션되지만 페이지 자체는 표시되지 않습니다.

이 상황은 WLC 문제(버그) 또는 클라이언트 측 문제일 가능성이 높습니다. 클라이언트에 방화벽 또는 소프트웨어 또는 정책 차단이 있을 수 있습니다. 또한 웹 브라우저에서 프록시를 구성했을 수도 있습니다.

권장 사항: 클라이언트 PC에서 스니퍼 추적을 수행합니다. 특별한 무선 소프트웨어는 필요하지 않습니다. 무선 어댑터에서 실행되고 WLC가 응답하고 리디렉션을 시도하는지 보여주는 Wireshark만 필요합니다. 다음과 같은 두 가지 가능성이 있습니다. WLC에서 응답이 없거나 WebAuth 페이지의 SSL 핸드셰이크에 문제가 있습니다. SSL 핸드셰이크 문제의 경우 사용자 브라우저에서 SSLv3을 허용하는지(일부는 SSLv2만 허용), 인증서 확인에 너무 적극적인 경우 확인할 수 있습니다.

웹 페이지가 DNS 없이 나타나는지 확인하기 위해 http://192.0.2.1을 수동으로 입력하는 것이 일반적인 단계입니다. 실제로 http://10.0.0.0을 입력하면 동일한 효과를 얻을 수 있습니다. WLC는 입력한 IP 주소를 리디렉션합니다. 따라서 http://192.0.2.1을 입력하면 웹 리디렉션 작업을 수행할 수 없습니다. https://192.0.2.1(보안)을 입력하면 WLC에서 HTTPS 트래픽을 리디렉션하지 않기 때문에 작동하지 않습니다(기본적으로 버전 8.0 이상에서는 가능합니다). 리디렉션 없이 페이지를 직접 로드하는 가장 좋은 방법은 https://192.0.2.1/login.html를 입력하는 것입니다.

- **사용자는 인증할 수 없습니다**.

  인증에 대해 설명하는 이 문서의 섹션을 참조하십시오. RADIUS에서 로컬로 자격 증명을 확인합니다.

- **사용자는 WebAuth를 통해 성공적으로 인증할 수 있지만 이후에는 인터넷에 액세스할 수 없습니다**.

  WLAN의 보안에서 WebAuth를 제거한 다음 열려 있는 WLAN을 가질 수 있습니다. 그런 다음 웹, DNS 등에 액세스할 수 있습니다. 또한 문제가 발생하면 WebAuth 설정을 모두 제거하고 인터페이스 컨피그레이션을 확인하십시오.

자세한 내용은 다음을 참조하십시오. WLC(Wireless LAN Controller)에서 웹 인증 문제 해결.

HTTP 프록시 서버 및 작동 방식

HTTP 프록시 서버를 사용할 수 있습니다. 클라이언트가 브라우저에 192.0.2.1이 프록시 서버를 거치지 않는다는 예외를 추가해야 하는 경우, WLC가 프록시 서버의 포트(일반적으로 8080)에서 HTTP 트래픽을 수신하도록 할 수 있습니다.

이 시나리오를 이해하려면 HTTP 프록시가 수행하는 작업을 알아야 합니다. 이는 브라우저의 클라이언트 측(IP 주소 및 포트)에서 구성하는 것입니다.

일반적으로 사용자가 웹 사이트를 방문할 때 DNS를 사용하여 이름을 IP로 확인한 다음 웹 서버에 웹 페이지를 묻는 것이 일반적인 시나리오입니다. 프로세스는 항상 페이지에 대한 HTTP 요청을 프록시로 전송합니다.

프록시는 필요한 경우 DNS를 처리하고 웹 서버에 전달합니다(페이지가 프록시에 아직 캐시되지 않은 경우). 토론은 클라이언트-프록시 전용입니다. 프록시가 실제 웹 페이지를 획득하는지 여부는 클라이언트와 무관하다.

다음은 웹 인증 프로세스입니다.

- URL에 사용자 유형을 입력합니다.
- 클라이언트 PC가 프록시 서버로 전송합니다.
- WLC가 프록시 서버 IP를 가로채고 모방합니다. 192.0.2.1로 리디렉션하여 PC에 응답합니다.

이 단계에서 PC가 구성되지 않은 경우 프록시에 192.0.2.1 WebAuth 페이지를 요청하여 작동하지 않습니다. PC는 192.0.2.1에 대한 예외를 만들어야 합니다. 그런 다음 HTTP 요청을 192.0.2.1로 전송하고 WebAuth를 진행합니다.

인증되면 모든 통신이 프록시를 다시 통과합니다. 예외 컨피그레이션은 일반적으로 프록시 서버의 컨피그레이션에 가까운 브라우저에 표시됩니다. 그러면 다음과 같은 메시지가 표시됩니다. "해당 IP 주소에 프록시를 사용하지 마십시오."

WLC 릴리스 7.0 이상에서는 **webauth proxy redirect** 전역 WLC 컨피그레이션 옵션에서 활성화할 수 있습니다.

활성화된 경우 WLC는 클라이언트가 프록시를 수동으로 사용하도록 구성되어 있는지 확인합니다. 이 경우 모든 것이 작동하도록 프록시 설정을 수정하는 방법을 보여 주는 페이지로 클라이언트를 리디렉션합니다.

WebAuth 프록시 리디렉션은 다양한 포트에서 작동하도록 구성할 수 있으며 중앙 웹 인증과 호환됩니다.

WebAuth 프록시 리디렉션의 예는 무선 LAN 컨트롤러 컨피그레이션 예제의 웹 인증 프록시를 참조하십시오.

HTTPS 대신 HTTP에 대한 웹 인증

HTTPS 대신 HTTP에서 웹 인증에 로그인할 수 있습니다. HTTP에서 로그인하면 인증서 알림을 받지 않습니다.

WLC 릴리스 7.2 코드 이전의 경우 WLC의 HTTPS 관리를 비활성화하고 HTTP 관리를 종료해야 합니다. 그러나 HTTP를 통한 WLC의 웹 관리만 허용됩니다.

WLC 릴리스 7.2 코드의 경우 **config network web-auth secureweb disable** 명령을 사용하여 비활성화합니다. 이렇게 하면 웹 인증에 대한 HTTPS만 비활성화되고 관리는 비활성화되지 않습니다. 컨트롤러를 재부팅해야 합니다.

WLC 릴리스 7.3 이상 코드에서는 GUI 및 CLI를 통해서만 WebAuth에 대해 HTTPS를 활성화/비활성화할 수 있습니다.

관련 정보

- Wireless LAN Controller 웹 인증 컨피그레이션 예
- 무선 컨트롤러용 소프트웨어 다운로드 WebAuth 번들
- 사용자 지정 웹 인증 로그인 페이지 생성
- 무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예
- Wireless LAN Controller 5760/3850 Web Passthrough 컨피그레이션 예
- 웹 리디렉션 구성(GUI)
- 웹 리디렉션 구성(CLI)
- WLC(Wireless LAN Controller)에서 웹 인증 문제 해결
- 무선 LAN 컨트롤러 컨피그레이션의 웹 인증 프록시 예
- RFC(설명 요청)
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.