WLC(Wireless LAN Controller)에서 웹 인증 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[관련 제품](#)
[WLC의 웹 인증](#)
[웹 인증 문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 WLC(Wireless LAN Controller) 환경에서 웹 인증 문제를 해결하기 위한 팁에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CAPWAP(Control and Provisioning of Wireless Access Point).
- 기본 작동을 위해 LAP(Lightweight Access Point) 및 WLC를 구성하는 방법.
- 웹 인증에 대한 기본 지식 및 WLC에서 웹 인증을 구성하는 방법.

WLC에서 웹 인증을 구성하는 방법에 대한 자세한 내용은 [무선 LAN 컨트롤러 웹 인증 컨피그레이션 예를 참조하십시오](#).

사용되는 구성 요소

이 문서의 정보는 펌웨어 버전 8.3.121을 실행하는 WLC 5500을 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.

관련 제품

이 문서는 다음 하드웨어와 함께 사용할 수도 있습니다.

- Cisco 5500 Series 무선 컨트롤러
- Cisco 8500 Series 무선 컨트롤러
- Cisco 2500 Series 무선 컨트롤러

- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Flex 7500 Series Wireless Controller
- Cisco WiSM2(Wireless Services Module 2)

WLC의 웹 인증

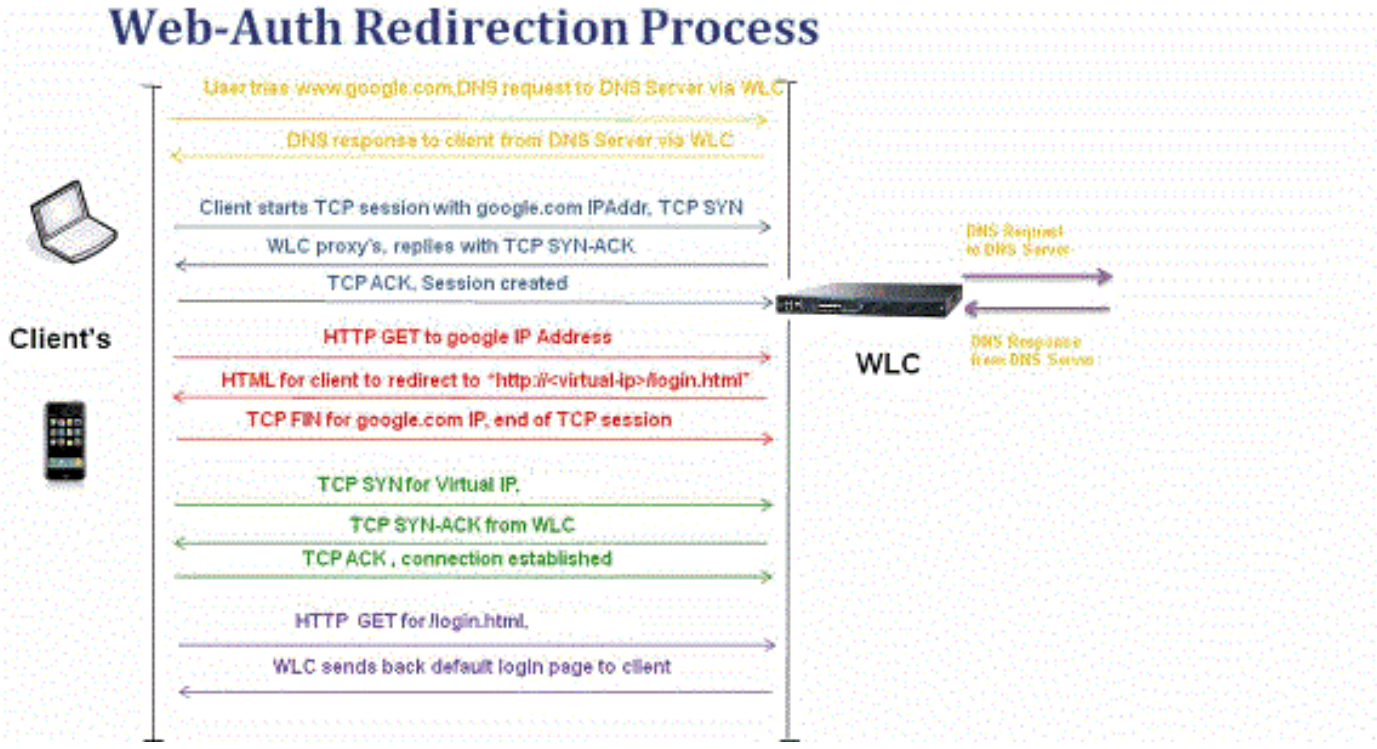
웹 인증은 컨트롤러가 특정 클라이언트의 IP 트래픽(DHCP 관련 패킷/DNS(Domain Name System) 관련 패킷 제외)을 허용하지 않도록 하는 레이어 3 보안 기능이며, 클라이언트가 올바른 사용자 이름 및 비밀번호를 올바르게 제공하도록 해야 합니다. 단, 사전 인증 ACL(Access Control List)을 통해 허용되는 트래픽은 예외입니다. 웹 인증은 인증 전에 클라이언트가 IP 주소를 가져올 수 있는 유일한 보안 정책입니다. 서 플리 컨 트 또는 클라이언트 유틸리티가 필요 없는 간단한 인증 방법입니다. 웹 인증은 WLC에서 로컬로 또는 RADIUS 서버를 통해 수행할 수 있습니다. 웹 인증은 일반적으로 게스트 액세스 네트워크를 구축하려는 고객이 사용합니다.

웹 인증은 컨트롤러가 클라이언트에서 첫 번째 TCP HTTP(포트 80) GET 패킷을 가로챌 때 시작됩니다. 클라이언트 웹 브라우저에서 이 범위를 확인하려면 클라이언트가 먼저 IP 주소를 얻고 웹 브라우저에 대한 URL을 IP 주소로 변환(DNS 확인)해야 합니다. 이렇게 하면 웹 브라우저가 HTTP GET을 전송할 IP 주소를 알 수 있습니다.

WLAN에 웹 인증이 구성된 경우 컨트롤러는 DHCP 및 DNS 트래픽을 제외하고 클라이언트에서 오는 모든 트래픽(인증 프로세스가 완료될 때까지)을 차단합니다. 클라이언트가 첫 번째 HTTP GET을 TCP 포트 80으로 전송하면 컨트롤러는 처리를 위해 클라이언트를 https://192.0.2.1/login.html(구성된 가상 IP인 경우)으로 리디렉션합니다. 이 프로세스는 결국 로그인 웹 페이지를 표시합니다.

> **참고**: 웹 인증에 외부 웹 서버를 사용할 경우 WLC 플랫폼에는 외부 웹 서버에 대한 사전 인증 ACL이 필요합니다.

이 섹션에서는 웹 인증 리디렉션 프로세스에 대해 자세히 설명합니다.



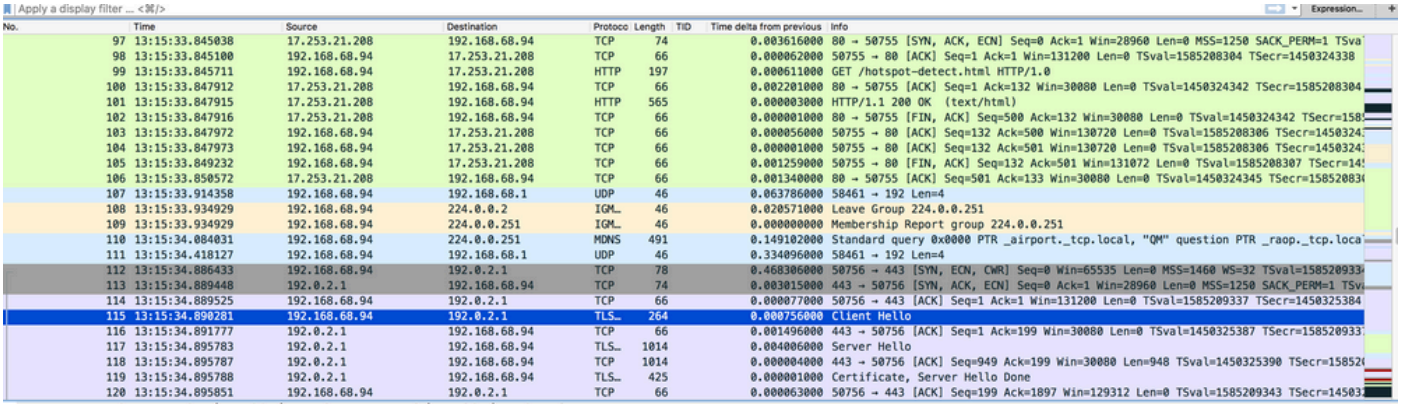
- 웹 브라우저를 열고 URL(예: http://www.site.com)을 입력합니다. 클라이언트는 대상의 IP를 가져오기 위해 이 URL에 대한 DNS 요청을 보냅니다. WLC는 DNS 요청을 DNS 서버로 전달하고 DNS 서버는 DNS 회신으로 응답합니다. DNS 회신에는 대상 www.site.com의 IP 주소가 포함되며, 이 주소는 무선 클라이언트로 전달됩니다.
- 그런 다음 클라이언트는 대상 IP 주소로 TCP 연결을 열려고 시도합니다. IP 주소 www.site.com으로 향하는 TCP SYN 패킷을 전송합니다.
- WLC에는 클라이언트에 대해 구성된 규칙이 있으므로 www.site.com에 대한 프록시 역할을 할 수 있습니다. TCP SYN-ACK 패킷을 클라이언트로 다시 전송합니다. 이때 소스는 IP 주소 www.site.com입니다. 클라이언트는 3방향 TCP 핸드셰이크를 완료하기 위해 TCP ACK 패킷을 다시 전송하고 TCP 연결이 완전히 설정됩니다.
- 클라이언트는 www.site.com으로 향하는 HTTP GET 패킷을 전송합니다. WLC가 이 패킷을 가로채서 리디렉션 처리를 위해 전송합니다. HTTP 애플리케이션 게이트웨이는 HTML 본문을 준비하고 클라이언트가 요청한 HTTP GET에 대한 응답으로 다시 전송합니다. 이 HTML을 사용하면 클라이언트가 WLC의 기본 웹 페이지 URL(예: http://<Virtual-Server-IP>/login.html)로 이동합니다.
- 클라이언트는 IP 주소(예: www.site.com)를 사용하여 TCP 연결을 닫습니다.
- 이제 클라이언트가 http://<virtualip>/login.html으로 이동하려고 하므로 WLC의 가상 IP 주소로 TCP 연결을 열려고 시도합니다. 192.0.2.1에 대한 TCP SYN 패킷(여기서는 가상 IP)을 WLC에 전송합니다.
- WLC는 TCP SYN-ACK로 응답하고 클라이언트는 핸드셰이크를 완료하기 위해 TCP ACK를 WLC에 다시 보냅니다.
- 클라이언트는 로그인 페이지를 요청하기 위해 192.0.2.1로 향하는 /login.html에 대한 HTTP GET을 전송합니다.
- 이 요청은 WLC의 웹 서버까지 허용되며 서버는 기본 로그인 페이지로 응답합니다. 클라이언트는 브라우저 창에서 로그인 페이지를 수신합니다. 여기서 사용자는 계속 로그인을 할 수 있습니다.

이 예에서 클라이언트 IP 주소는 192.168.68.94입니다. 클라이언트가 액세스한 웹 서버(10.1.0.13)의 URL을 확인했습니다. 보시다시피 클라이언트는 3방향 핸드셰이크를 수행하여 TCP 연결을 시작한 다음 패킷 96으로 시작된 HTTP GET 패킷을 전송했습니다(00은 HTTP 패킷). 이는 사용자에 의해 트리거된 것이 아니라 운영 체제 자동 포털 탐지 트리거였습니다(요청된 URL에서 추측할 수 있듯이). 컨트롤러는 패킷을 인터셉트하고 코드 200으로 회신한다. 코드 200 패킷에는 리디렉션 URL이 있습니다.

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

그런 다음 3방향 핸드셰이크를 통해 TCP 연결을 닫습니다.

그런 다음 클라이언트는 컨트롤러의 가상 IP 주소인 192.0.2.1로 전송하는 리디렉션 URL에 대한 HTTPS 연결을 시작합니다. 클라이언트는 SSL 터널을 가져오기 위해 서버 인증서를 검증하거나 무시해야 합니다. 이 경우 자체 서명 인증서이므로 클라이언트가 무시했습니다. 로그인 웹 페이지는 이 SSL 터널을 통해 전송됩니다. 패킷 112는 트랜잭션을 시작합니다.



No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=145
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=158520836
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=158520
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=145032

WLC의 가상 IP 주소에 대한 도메인 이름을 구성하는 옵션이 있습니다. 가상 IP 주소에 대한 도메인 이름을 구성하는 경우, 이 도메인 이름은 클라이언트의 HTTP GET 패킷에 대한 응답으로 컨트롤러의 HTTP OK 패킷에 반환됩니다. 그런 다음 이 도메인 이름에 대해 DNS 확인을 수행해야 합니다. DNS 확인에서 IP 주소를 가져오면 컨트롤러의 가상 인터페이스에 구성된 IP 주소인 해당 IP 주소로 TCP 세션을 열려고 시도합니다.

결국 웹 페이지는 터널을 통해 클라이언트로 전달되며 사용자는 SSL(Secure Sockets Layer) 터널을 통해 사용자 이름/비밀번호를 다시 전송합니다.

웹 인증은 다음 세 가지 방법 중 하나로 수행됩니다.

- 내부 웹 페이지를 사용합니다(기본값).
- 사용자 지정 로그인 페이지를 사용합니다.
- 외부 웹 서버의 로그인 페이지를 사용합니다.

참고:
- 사용자 지정 웹 인증 번들의 파일 이름은 최대 30자로 제한됩니다. 번들 내 파일 이름이 30자를 초과하지 않는지 확인합니다.

- WLC 릴리스 7.0 이후부터는 WLAN에서 웹 인증이 활성화되고 CPU ACL 규칙도 있는 경우 클라이언트가 WebAuth_Reqd 상태에서 인증되지 않은 한 클라이언트 기반 웹 인증 규칙이 항상 더 높은 우선 순위를 갖습니다. 클라이언트가 RUN 상태로 전환되면 CPU ACL 규칙이 적용됩니다.

- 따라서 CPU ACL이 WLC에서 활성화된 경우 다음 조건에서 가상 인터페이스 IP에 대한 허용 규칙이 필요합니다(모든 방향).
 - CPU ACL에 양방향 모두 허용 규칙이 없는 경우.
 - ALLOW ALL(모두 허용) 규칙이 있지만, 우선순위가 더 높은 포트 443 또는 80에 대한 DENY 규칙도 있는 경우.

- 가상 IP에 대한 허용 규칙은 secureweb이 비활성화된 경우 TCP 프로토콜 및 포트 80, secureweb이 활성화된 경우 포트 443이어야 합니다. 이는 CPU ACL이 있을 때 성공 적 인 인증 후 가상 인터페이스 IP 주소에 클라이언트의 액세스를 허용 하기 위해 필요 합니다.

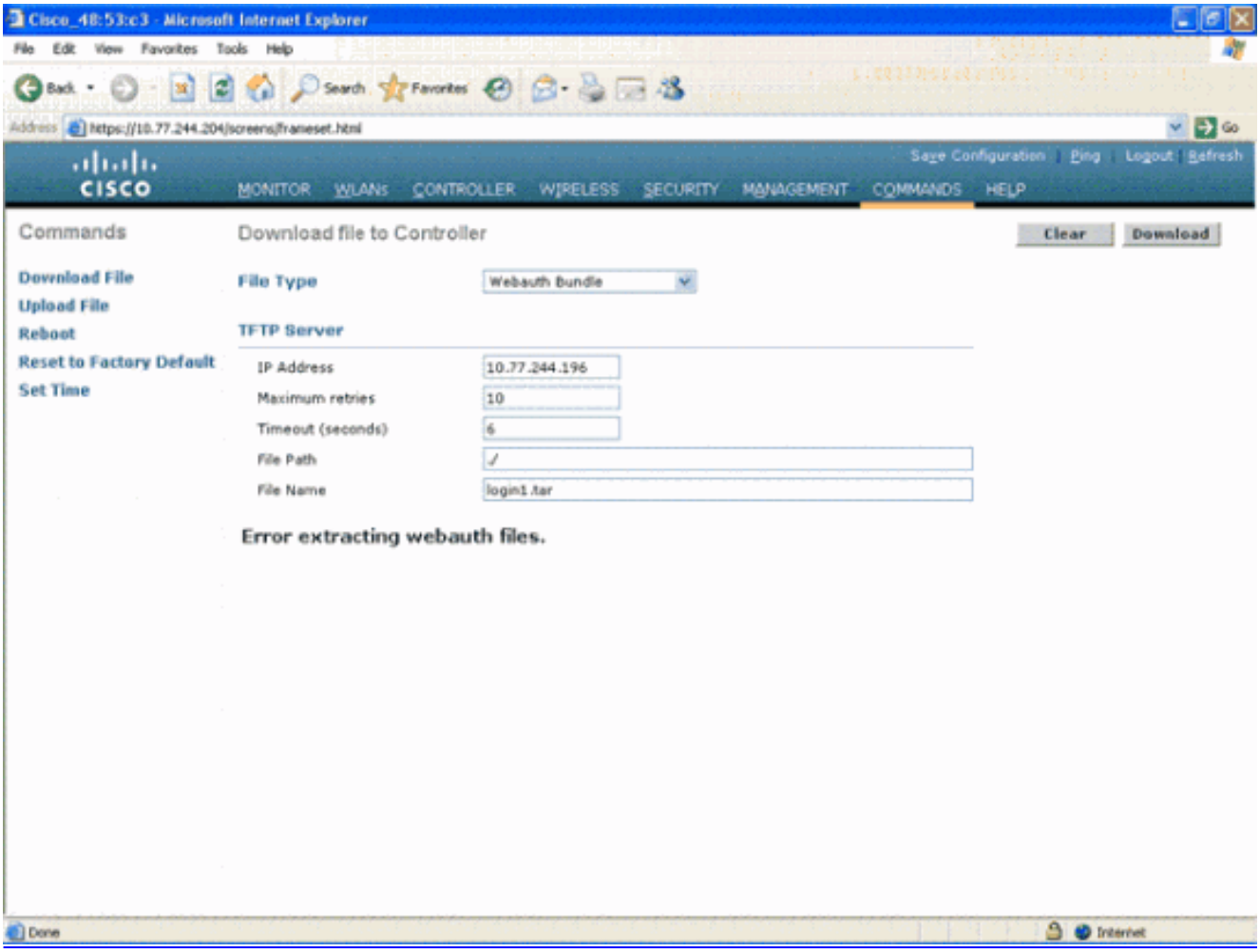
웹 인증 문제 해결

웹 인증을 구성하고 기능이 예상대로 작동하지 않으면 다음 단계를 완료합니다.

1. 클라이언트가 IP 주소를 받는지 확인합니다. 그렇지 않은 경우 사용자는 WLAN에서 DHCP **Required(DHCP** 필수) 확인란의 선택을 취소하고 무선 클라이언트에 고정 IP 주소를 제공할

수 있습니다. 이는 액세스 포인트와의 연계를 전제로 합니다.

2. 프로세스의 다음 단계는 웹 브라우저에서 URL의 DNS 확인입니다. WLAN 클라이언트가 웹 인증을 위해 구성된 WLAN에 연결되면 클라이언트는 DHCP 서버에서 IP 주소를 가져옵니다. 사용자가 웹 브라우저를 열고 웹 사이트 주소를 입력합니다. 클라이언트는 웹 사이트의 IP 주소를 얻기 위해 DNS 확인을 수행합니다. 이제 클라이언트가 웹 사이트에 연결하려고 하면 WLC는 클라이언트의 HTTP GET 세션을 가로채고 사용자를 웹 인증 로그인 페이지로 리디렉션합니다.
3. 따라서 클라이언트가 리디렉션이 작동하도록 DNS 확인을 수행할 수 있어야 합니다. Microsoft Windows에서 **Start(시작) > Run(실행)을** 선택하고, **명령 창**을 열려면 CMD를 입력한 다음 "nslookup www.cisco.com"을 수행하여 IP 주소가 복구되는지 확인합니다. Mac/Linux에서 터미널 창을 열고 "nslookup www.cisco.com"을 수행하고 IP 주소가 다시 나타나는지 확인합니다.클라이언트가 DNS 확인을 받지 못한다고 생각되면 다음 중 하나를 수행할 수 있습니다 .URL의 IP 주소를 입력합니다(예: http://www.cisco.com은 http://192.168.219.25임).무선 어댑터를 통해 확인해야 하는 모든(존재하지 않는) IP 주소를 입력해 보십시오.이 URL을 입력하면 웹 페이지가 표시됩니까? 대답이 "예"인 경우 DNS 문제일 가능성이 높습니다. 인증서 문제일 수도 있습니다. 기본적으로 컨트롤러는 자체 서명 인증서를 사용하며 대부분의 웹 브라우저는 사용을 경고합니다.
4. 사용자 지정 웹 페이지를 사용한 웹 인증의 경우 사용자 지정 웹 페이지의 HTML 코드가 적절한지 확인합니다. Cisco 소프트웨어 다운로드에서 샘플 웹 인증 스크립트를 다운로드할 수 있습니다. 예를 들어, 5508 컨트롤러의 경우 **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundle을** 선택하고 webauth_**bundle.zip 파일을** 다운로드합니다.이러한 매개변수는 사용자의 인터넷 브라우저가 사용자 지정 로그인 페이지로 리디렉션될 때 URL에 추가됩니다.ap_mac - 무선 사용자가 연결된 액세스 포인트의 MAC 주소입니다.switch_url - 사용자 자격 증명을 게시해야 하는 컨트롤러의 URL입니다.redirect - 인증에 성공한 후 사용자가 리디렉션되는 URL입니다.statusCode - 컨트롤러 웹 인증 서버에서 반환된 상태 코드입니다.wlan - 무선 사용자가 연결된 WLAN SSID입니다.사용 가능한 상태 코드는 다음과 같습니다.상태 코드 1 - "이미 로그인되었습니다. 더 이상의 조치가 필요하지 않습니다."상태 코드 2 - "웹 포털에 대해 인증하도록 구성되지 않았습니다. 더 이상의 조치가 필요하지 않습니다."상태 코드 3 - "현재 지정된 사용자 이름을 사용할 수 없습니다. 사용자 이름이 이미 시스템에 로그인되어 있을 수 있습니다."상태 코드 4 - "제외되었습니다."상태 코드 5 - "입력한 사용자 이름 및 암호 조합이 잘못되었습니다. 다시 시도하십시오."
5. 사용자 지정 웹 페이지에 표시해야 하는 모든 파일 및 사진은 WLC에 업로드되기 전에 .tar 파일에 번들로 묶어야 합니다. .tar 번들에 포함된 파일 중 하나가 login.html인지 확인합니다. login.html 파일을 포함하지 않으면 다음과 같은 오류 메시지가 표시됩니다.



사용자 지정 웹 인증 창을 만드는 방법에 대한 자세한 내용은 Wireless LAN Controller 웹 인증 구성 예의 사용자 지정 웹 인증 지침 섹션을 참조하십시오.**참고**: 크기가 큰 파일과 이름이 긴 파일은 추출 오류가 발생할 수 있습니다. 사진은 .jpg 형식으로 표시하는 것이 좋습니다.

6. WLC의 **사용자** 지정 웹 페이지가 기본적으로 HTML 스크립트이므로 클라이언트 브라우저에서 Scripting 옵션이 차단되지 않았는지 확인합니다.
7. WLC의 **가상 인터페이스**에 대해 구성된 **호스트 이름**이 있는 경우 가상 인터페이스의 호스트 이름에 대해 DNS 확인을 사용할 수 있는지 확인합니다. **참고**: **DNS** 호스트 이름을 가상 **인터페이스**에 할당하려면 WLC GUI에서 Controller(컨트롤러) > Interfaces(인터페이스) **메뉴**로 이동합니다.
8. 클라이언트 컴퓨터에 설치된 방화벽이 웹 인증 로그인 페이지를 차단하는 경우가 있습니다. 로그인 페이지에 액세스하기 전에 방화벽을 비활성화합니다. 웹 인증이 완료되면 방화벽을 다시 활성화할 수 있습니다.
9. 토폴로지/솔루션 방화벽은 클라이언트와 웹 인증 서버 사이에 위치할 수 있으며, 웹 인증 서버는 네트워크에 따라 달라집니다. 구현된 각 네트워크 설계/솔루션에 대해 최종 사용자는 네트워크 방화벽에서 이러한 포트가 허용되는지 확인해야 합니다.

10. 웹 인증이 발생하려면 먼저 클라이언트가 WLC의 해당 WLAN에 연결되어야 합니다. 클라이언트가 WLC에 **연결되었는지** 확인하려면 WLC GUI에서 Monitor(모니터) > Clients(클라이언트) 메뉴로 이동합니다. 클라이언트에 유효한 IP 주소가 있는지 확인합니다.
11. 웹 인증이 완료될 때까지 클라이언트 브라우저에서 프록시 설정을 비활성화합니다.
12. 기본 웹 인증 방법은 PAP(Password Authentication Protocol)입니다. RADIUS 서버에서 PAP 인증이 허용되는지 확인합니다. 클라이언트 인증의 상태를 확인하려면 RADIUS 서버에서 디버깅 및 로그 메시지를 확인 하십시오. RADIUS 서버에서 **디버그를** 보려면 WLC에서 debug aaa all 명령을 사용할 수 있습니다.

13. 컴퓨터의 하드웨어 드라이버를 제조업체 웹 사이트의 최신 코드로 업데이트합니다.
14. 신청자(랩톱의 프로그램)에서 설정을 확인합니다.
15. Windows에 내장된 Windows Zero Config 신청자를 사용하는 경우: 사용자에게 최신 패치가 설치되어 있는지 확인합니다.신청자에서 디버그를 실행합니다.
16. 클라이언트에서 명령 창에서 EAPOL(WPA+WPA2) 및 RASTLS 로그를 켭니다. 시작 **> 실행 > CMD를 선택 합니다**.
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    로그를 비활성화하려면 동일한 명령을 실행하되 enable을 disable로 바꿉니다. XP의 경우 모든 로그는 C:\Windows\tracing에 있을 수 있습니다.
17. 로그인 웹 페이지가 아직 없는 경우 단일 클라이언트에서 이 출력을 수집하고 분석합니다.
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. 이 단계를 완료한 후에도 문제가 해결되지 않으면 이러한 디버그를 수집하고 Support Case Manager를 사용하여 서비스 요청을 엽니다.
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

관련 정보

- Wireless LAN Controller 웹 인증 컨피그레이션 예
- Wireless LAN Controller를 사용한 외부 웹 인증 컨피그레이션 예
- 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.