Fehlerbehebung für die Webauthentifizierung auf einem Wireless LAN Controller (WLC)

Inhalt

Einleitung

In diesem Dokument werden Tipps zur Behebung von Web-Authentifizierungsproblemen in einer Wireless LAN Controller (WLC)-Umgebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CAPWAP (Control and Provisioning of Wireless Access Points)
- Konfigurieren von Lightweight Access Point (LAP) und WLC für den Basisbetrieb
- Grundkenntnisse der Webauthentifizierung und der Konfiguration der Webauthentifizierung auf WLCs

Weitere Informationen zum Konfigurieren der Webauthentifizierung auf WLCs finden Sie unter Konfigurationsbeispiel für die Webauthentifizierung des Wireless LAN-Controllers.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem WLC 5500 mit der Firmware-Version 8.3.121.

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgender Hardware verwendet werden:

- Cisco Wireless-Controller der Serie 5500
- Cisco Wireless Controller der Serie 8500
- Cisco Wireless Controller der Serie 2500
- Cisco Airespace WLAN-Controller der Serie 3500
- Cisco Airespace Wireless LAN Controller der Serie 4000
- Cisco Flex Wireless Controller der Serie 7500
- Cisco Wireless Services Module 2 (WiSM2)

Webauthentifizierung auf WLCs

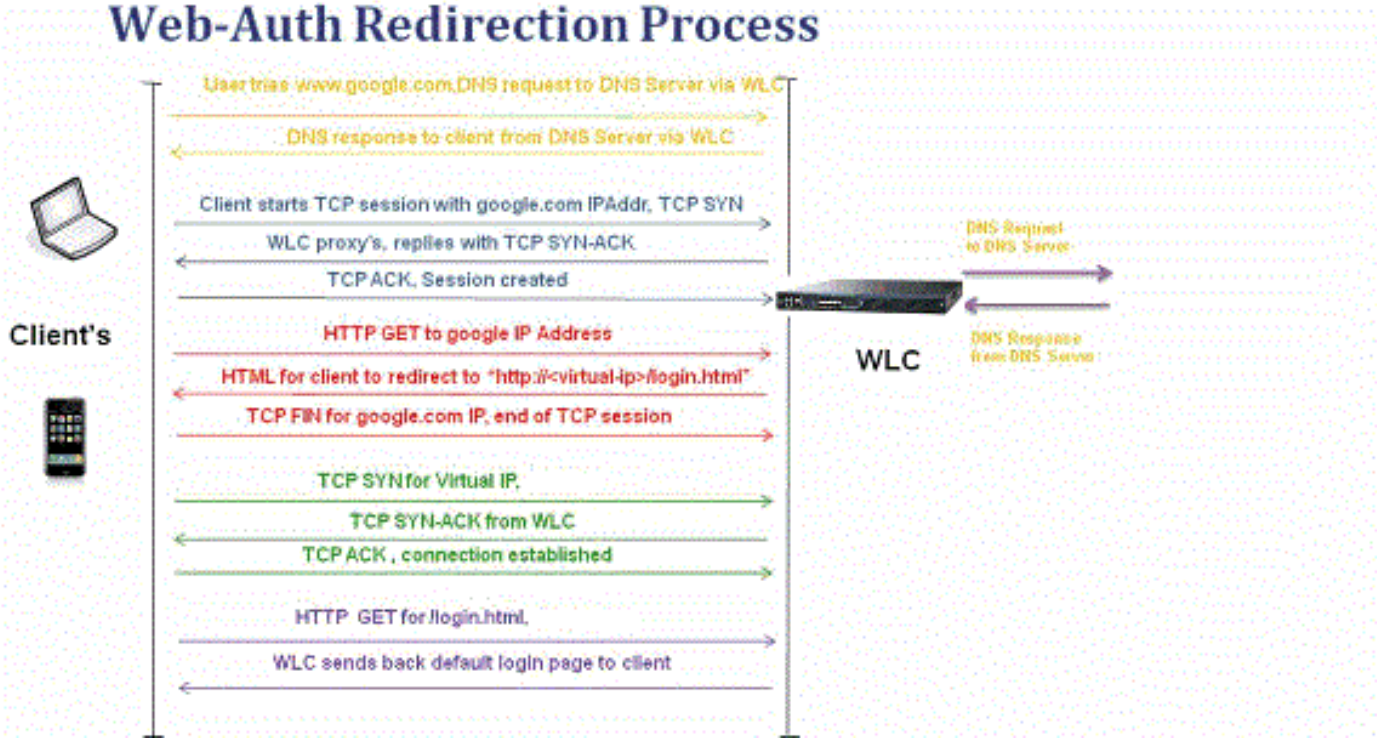
Die Webauthentifizierung ist eine Layer-3-Sicherheitsfunktion, die den Controller veranlasst, IP-Datenverkehr, ausgenommen DHCP-bezogene Pakete/DNS-bezogene Pakete (Domain Name System), von einem bestimmten Client erst dann zuzulassen, wenn dieser Client korrekt einen gültigen Benutzernamen und ein gültiges Kennwort angegeben hat, mit Ausnahme des Datenverkehrs, der über eine Pre-Auth-Zugriffskontrollliste (ACL) zugelassen wird. Die Webauthentifizierung ist die einzige Sicherheitsrichtlinie, die dem Client den Abruf einer IP-Adresse vor der Authentifizierung ermöglicht. Es handelt sich um eine einfache Authentifizierungsmethode, ohne dass eine Komponente oder ein Client-Dienstprogramm erforderlich ist. Die Webauthentifizierung kann entweder lokal auf einem WLC oder über einen RADIUS-Server erfolgen. Die Webauthentifizierung wird in der Regel von Kunden verwendet, die ein Gastzugriffsnetzwerk bereitstellen möchten.

Die Webauthentifizierung beginnt, wenn der Controller das erste TCP HTTP (Port 80) GET-Paket vom Client abfängt. Damit der Client-Webbrowser so weit kommt, muss der Client zunächst eine IP-Adresse erhalten und eine Übersetzung der URL in eine IP-Adresse (DNS-Auflösung) für den Webbrowser vornehmen. Dadurch wird dem Webbrowser mitgeteilt, welche IP-Adresse HTTP GET senden soll.

Wenn die Webauthentifizierung im WLAN konfiguriert ist, blockiert der Controller den gesamten Datenverkehr vom Client (bis der Authentifizierungsprozess abgeschlossen ist), mit Ausnahme des DHCP- und DNS-Datenverkehrs. Wenn der Client das erste HTTP GET an den TCP-Port 80 sendet, leitet der Controller den Client zur Verarbeitung an https://192.0.2.1/login.html (wenn dies die konfigurierte virtuelle IP ist) weiter. Dieser Prozess öffnet schließlich die Anmelde-Webseite.

> **Hinweis**: Wenn Sie einen externen Webserver für die Webauthentifizierung verwenden, benötigen WLC-Plattformen eine ACL vor der Authentifizierung für den externen Webserver.

In diesem Abschnitt wird der Prozess der Webauthentifizierungsumleitung ausführlich erläutert.



- Sie öffnen den Webbrowser und geben eine URL ein, z. B. http://www.site.com. Der Client sendet eine DNS-Anforderung für diese URL, um die IP-Adresse für das Ziel abzurufen. WLC gibt die DNS-Anfrage an den DNS-Server weiter und der DNS-Server antwortet mit einer DNS-Antwort, die die IP-Adresse des Ziels www.site.com enthält, die wiederum an die Wireless-Clients weitergeleitet wird.
- Der Client versucht dann, eine TCP-Verbindung mit der Ziel-IP-Adresse zu öffnen. Es sendet ein TCP-SYN-Paket an die IP-Adresse von www.site.com.
- Der WLC verfügt über Regeln, die für den Client konfiguriert sind, und kann daher als Proxy für www.site.com fungieren. Es sendet ein TCP-SYN-ACK-Paket zurück an den Client, dessen Quelle die IP-Adresse www.site.com ist. Der Client sendet ein TCP-ACK-Paket zurück, um den Drei-Wege-TCP-Handshake abzuschließen, und die TCP-Verbindung ist vollständig hergestellt.
- Der Client sendet ein HTTP GET-Paket an www.site.com. Der WLC fängt dieses Paket ab und sendet es zur Weiterleitungsbehandlung. Das HTTP-Anwendungs-Gateway bereitet einen HTML-Text vor und sendet diesen als Antwort auf die vom Client angeforderte HTTP GET-Anforderung zurück. Dieser HTML-Code veranlasst den Client, zur Standard-Webseite-URL des WLC zu wechseln, z. B. http://<Virtual-Server-IP>/login.html.
- Der Client schließt die TCP-Verbindung mit der IP-Adresse, z. B. www.site.com.
- Nun möchte der Client auf http://<virtualip>/login.html gehen und versucht, eine TCP-Verbindung mit der virtuellen IP-Adresse des WLC zu öffnen. Es sendet ein TCP-SYN-Paket für 192.0.2.1 (die virtuelle IP hier) an den WLC.
- Der WLC antwortet mit einem TCP SYN-ACK und der Client sendet ein TCP ACK zurück an den WLC, um den Handshake abzuschließen.
- Der Client sendet ein HTTP GET für /login.html, das für 192.0.2.1 bestimmt ist, um die Anmeldeseite anzufordern.
- Diese Anforderung ist bis zum Webserver des WLC zulässig, und der Server antwortet mit der Standardanmeldeseite. Der Client erhält die Anmeldeseite im Browserfenster, auf der sich der Benutzer anmelden kann.

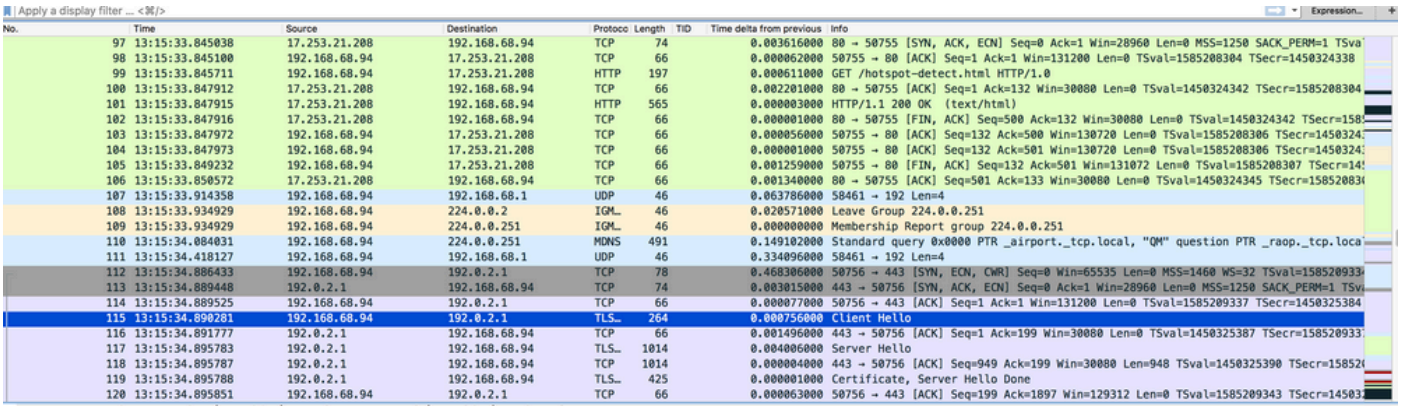
In diesem Beispiel ist die Client-IP-Adresse 192.168.68.94. Der Client hat die URL zu dem

Webserver aufgelöst, auf den zugegriffen wurde, 10.1.0.13. Wie Sie sehen, hat der Client den Drei-Wege-Handshake durchgeführt, um die TCP-Verbindung zu starten, und hat dann ein HTTP GET-Paket gesendet, das mit Paket 96 (00 ist das HTTP-Paket) begonnen hat. Dies wurde nicht vom Benutzer ausgelöst, sondern durch die automatische Portalerkennung des Betriebssystems (wie wir an der angeforderten URL erraten können). Der Controller fängt die Pakete ab und antwortet mit Code 200. Das Code-200-Paket enthält eine Umleitungs-URL:

```
<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>
```

Anschließend wird die TCP-Verbindung durch einen Drei-Wege-Handshake geschlossen.

Der Client startet dann die HTTPS-Verbindung zur Umleitungs-URL, die sie an 192.0.2.1 sendet, die virtuelle IP-Adresse des Controllers. Der Client muss das Serverzertifikat validieren oder ignorieren, um den SSL-Tunnel zu öffnen. In diesem Fall handelt es sich um ein selbstsigniertes Zertifikat, das vom Client ignoriert wurde. Die Anmelde-Webseite wird über diesen SSL-Tunnel gesendet. Paket 112 beginnt mit den Transaktionen.



No.	Time	Source	Destination	Protoco	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=14503

Sie haben die Möglichkeit, den Domänennamen für die virtuelle IP-Adresse des WLC zu konfigurieren. Wenn Sie den Domänennamen für die virtuelle IP-Adresse konfigurieren, wird dieser Domänenname im HTTP-OK-Paket vom Controller als Antwort auf das HTTP-GET-Paket vom Client zurückgegeben. Anschließend müssen Sie eine DNS-Auflösung für diesen Domänennamen durchführen. Sobald er eine IP-Adresse aus der DNS-Auflösung bezieht, versucht er, eine TCP-Sitzung mit dieser IP-Adresse zu öffnen. Dabei handelt es sich um eine IP-Adresse, die auf einer virtuellen Schnittstelle des Controllers konfiguriert wurde.

Schließlich wird die Webseite durch den Tunnel zum Client geleitet, und der Benutzer sendet Benutzername/Kennwort über den SSL-Tunnel (Secure Sockets Layer) zurück.

Die Webauthentifizierung wird mit einer der folgenden drei Methoden durchgeführt:

- Verwenden Sie eine interne Webseite (Standard).
- Benutzerdefinierte Anmeldeseite verwenden.
- Verwenden Sie eine Anmeldeseite von einem externen Webserver.

Hinweise:
- Das benutzerdefinierte Web-Authentifizierungspaket darf maximal 30 Zeichen für

Dateinamen enthalten. Stellen Sie sicher, dass keine Dateinamen im Paket mehr als 30 Zeichen enthalten.

- Ab WLC Version 7.0 haben, wenn die Webauthentifizierung im WLAN aktiviert ist und Sie außerdem CPU-ACL-Regeln haben, die clientbasierten Webauthentifizierungsregeln immer eine höhere Priorität, solange der Client im WebAuth_Reqd-Status nicht authentifiziert ist. Sobald der Client in den Status "RUN" wechselt, werden CPU-ACL-Regeln angewendet.

- Wenn CPU-ACLs im WLC aktiviert sind, ist daher unter den folgenden Bedingungen eine Zulassungsregel für die IP der virtuellen Schnittstelle (in BELIEBIGE Richtung) erforderlich:
 - Wenn die CPU-ACL über keine "Alle zulassen"-Regel für beide Richtungen verfügt.
 - Wenn eine "Alle zulassen"-Regel vorhanden ist, aber auch eine "Ablehnen"-Regel für Port 443 oder 80 mit höherer Priorität.

- Die Zulassungsregel für die virtuelle IP muss für das TCP-Protokoll und Port 80 sein, wenn SecureWeb deaktiviert ist, oder Port 443, wenn SecureWeb aktiviert ist. Dies ist erforderlich, damit der Client nach erfolgreicher Authentifizierung auf die IP-Adresse der virtuellen Schnittstelle zugreifen kann, wenn CPU-Zugriffskontrolllisten vorhanden sind.

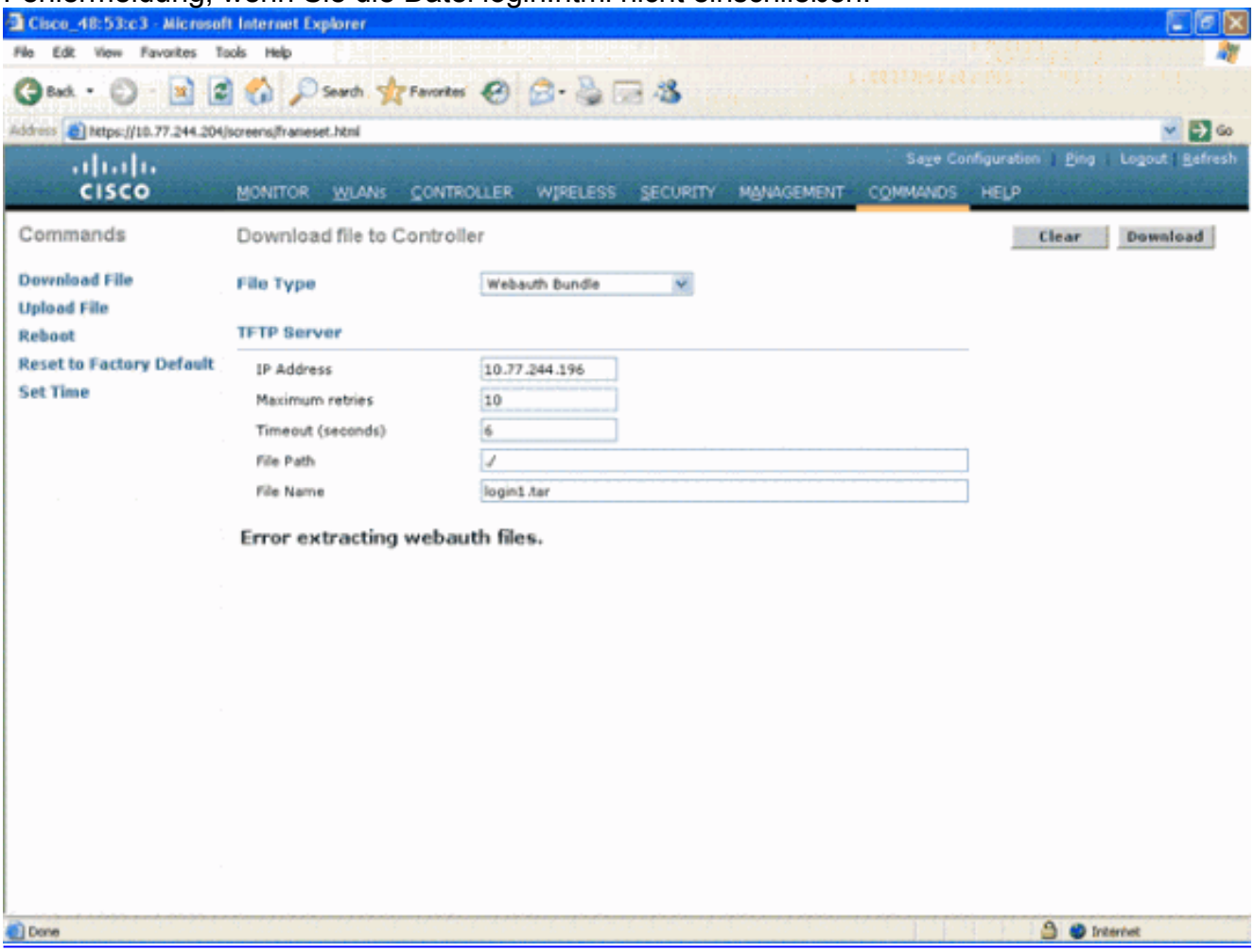
Problembehandlung bei der Webauthentifizierung

Führen Sie nach der Konfiguration der Webauthentifizierung die folgenden Schritte aus, wenn die Funktion nicht wie erwartet funktioniert:

1. Überprüfen Sie, ob der Client eine IP-Adresse erhält. Ist dies nicht der Fall, können Benutzer das Kontrollkästchen **DHCP erforderlich** im WLAN deaktivieren und dem Wireless-Client eine statische IP-Adresse zuweisen. Dies setzt eine Verknüpfung mit dem Access Point voraus.
2. Der nächste Schritt dabei ist die DNS-Auflösung der URL im Webbrowser. Wenn ein WLAN-Client eine Verbindung zu einem für die Webauthentifizierung konfigurierten WLAN herstellt, erhält der Client eine IP-Adresse vom DHCP-Server. Der Benutzer öffnet einen Webbrowser und gibt eine Website-Adresse ein. Der Client führt dann die DNS-Auflösung aus, um die IP-Adresse der Website zu erhalten. Wenn der Client jetzt versucht, die Website zu erreichen, fängt der WLC die HTTP GET-Sitzung des Clients ab und leitet den Benutzer zur Anmeldeseite für die Webauthentifizierung um.
3. Stellen Sie deshalb sicher, dass der Client eine DNS-Auflösung durchführen kann, damit die Umleitung funktioniert. Wählen Sie in Microsoft Windows **Start > Ausführen,** geben Sie **CMD** ein, um ein Befehlsfenster zu öffnen, und führen Sie einen "nslookup www.cisco.com" aus, und prüfen Sie, ob die IP-Adresse wieder angezeigt wird. Öffnen Sie unter Macs/Linux ein Terminalfenster, und führen Sie einen "nslookup www.cisco.com" aus, und überprüfen Sie, ob die IP-Adresse wieder angezeigt wird.Wenn Sie glauben, dass der Client keine DNS-Auflösung erhält, können Sie:Geben Sie entweder die IP-Adresse der URL ein (z. B. http://www.cisco.com ist http://192.168.219.25).Versuchen Sie, eine (auch nicht vorhandene) IP-Adresse einzugeben, die über den Wireless-Adapter aufgelöst werden muss.Wird die Webseite angezeigt, wenn Sie diese URL eingeben? Wenn ja, handelt es sich höchstwahrscheinlich um ein DNS-Problem. Es kann sich auch um ein Zertifikatproblem handeln. Der Controller verwendet standardmäßig ein selbstsigniertes Zertifikat, und die meisten Webbrowser warnen vor dessen Verwendung.
4. Bei der Webauthentifizierung mit einer angepassten Webseite stellen Sie sicher, dass der HTML-Code für die angepasste Webseite korrekt ist. Sie können ein Beispiel für ein Web-

Authentifizierungs-Skript von Cisco Software-Downloads herunterladen. Wählen Sie für die Controller der Serie 5508 beispielsweise **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 Bundle aus,** und laden Sie die Datei **webauth_bundle.zip** herunter.Diese Parameter werden der URL hinzugefügt, wenn der Internetbrowser des Benutzers auf die benutzerdefinierte Anmeldeseite umgeleitet wird:ap_mac - Die MAC-Adresse des Access Points, dem der Wireless-Benutzer zugeordnet ist.switch_url - Die URL des Controllers, an den die Benutzeranmeldeinformationen gesendet werden müssen.redirect - Die URL, zu der der Benutzer nach erfolgreicher Authentifizierung umgeleitet wird.statusCode - Der vom Webauthentifizierungsserver des Controllers zurückgegebene Statuscode.wlan - Die WLAN-SSID, der der Wireless-Benutzer zugeordnet ist.Folgende Statuscodes stehen zur Verfügung:Statuscode 1 - "Sie sind bereits angemeldet. Es sind keine weiteren Maßnahmen Ihrerseits erforderlich."Statuscode 2 - "Sie sind nicht für die Authentifizierung über das Webportal konfiguriert. Es sind keine weiteren Maßnahmen Ihrerseits erforderlich."Statuscode 3 - "Der angegebene Benutzername kann zurzeit nicht verwendet werden. Vielleicht ist der Benutzername bereits im System angemeldet?"Statuscode 4 - "Sie wurden ausgeschlossen."Statuscode 5 - "Die von Ihnen eingegebene Kombination aus Benutzername und Kennwort ist ungültig. Bitte versuchen Sie es erneut."

5. Alle Dateien und Bilder, die auf der angepassten Webseite erscheinen müssen, müssen in einer .tar-Datei gebündelt werden, bevor sie in den WLC hochgeladen werden. Stellen Sie sicher, dass login.html eine der im .tar-Paket enthaltenen Dateien ist. Sie erhalten diese Fehlermeldung, wenn Sie die Datei login.html nicht einschließen:



Weitere Informationen zum Erstellen eines benutzerdefinierten Web-

Authentifizierungsfensters finden Sie im Abschnitt Richtlinien für die benutzerdefinierte Web-Authentifizierung des Konfigurationsbeispiels für die Web-Authentifizierung des Wireless LAN-Controllers.**Hinweis**: Große Dateien und Dateien mit langen Namen können zu einem Extraktionsfehler führen. Es wird empfohlen, dass die Bilder im JPG-Format vorliegen.

6. Stellen Sie sicher, dass die **Scripting-**Option im Client-Browser nicht blockiert ist, da die angepasste Webseite im WLC im Grunde ein HTML-Skript ist.
7. Wenn Sie einen **Hostnamen** für die **virtuelle Schnittstelle** des WLC konfiguriert haben, stellen Sie sicher, dass die DNS-Auflösung für den Hostnamen der virtuellen Schnittstelle verfügbar ist. **Hinweis**: Navigieren Sie in der WLC-GUI zum Menü **Controller > Interfaces (Controller > Schnittstellen),** um der virtuellen Schnittstelle einen **DNS-Hostnamen** zuzuweisen.
8. Manchmal blockiert die auf dem Client-Computer installierte Firewall die Anmeldeseite für die Webauthentifizierung. Deaktivieren Sie die Firewall, bevor Sie auf die Anmeldeseite zugreifen. Die Firewall kann nach Abschluss der Webauthentifizierung wieder aktiviert werden.
9. Die Topologie-/Lösungs-Firewall kann zwischen dem Client und dem Web-Authentifizierungs-Server platziert werden, was vom Netzwerk abhängt. Wie bei jedem implementierten Netzwerkdesign/ jeder implementierten Lösung muss der Endbenutzer sicherstellen, dass diese Ports in der Netzwerk-Firewall zugelassen sind.

10. Damit die Webauthentifizierung durchgeführt werden kann, muss der Client zuerst eine Verbindung mit dem entsprechenden WLAN auf dem WLC herstellen. Navigieren Sie in der WLC-GUI zum Menü **Monitor > Clients** (**Überwachung > Clients**), um festzustellen, ob der Client mit dem WLC verbunden ist. Überprüfen Sie, ob der Client über eine gültige IP-Adresse verfügt.
11. Deaktivieren Sie die Proxyeinstellungen im Client-Browser, bis die Webauthentifizierung abgeschlossen ist.
12. Die Standard-Web-Authentifizierungsmethode ist das Password Authentication Protocol (PAP). Stellen Sie sicher, dass die PAP-Authentifizierung auf dem RADIUS-Server zugelassen ist, damit dies funktioniert. Um den Status der Client-Authentifizierung zu überprüfen, überprüfen Sie die Debug- und Protokollmeldungen des RADIUS-Servers. Sie können den Befehl **debug aaa all** auf dem WLC verwenden, um die Debugging-Meldungen vom RADIUS-Server anzuzeigen.
13. Aktualisieren Sie den Hardwaretreiber auf dem Computer auf den neuesten Code von der Website des Herstellers.
14. Überprüfen Sie die Einstellungen in der Komponente (Programm auf dem Laptop).
15. Wenn Sie die Windows Zero Config-Komponente verwenden, die in Windows integriert ist: Überprüfen Sie, ob der Benutzer über die neuesten Patches verfügt.Führen Sie Debug-Vorgänge für die Komponente aus.
16. Aktivieren Sie auf dem Client in einem Befehlsfenster die EAPOL- (WPA+WPA2) und RASTLS-Protokolle. Wählen Sie **Start > Ausführen > CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    Um die Protokolle zu deaktivieren, führen Sie den gleichen Befehl aus, ersetzen jedoch enable durch disable. Unter XP finden Sie alle Protokolle unter C:\Windows\tracing.
17. Wenn Sie immer noch keine Anmelde-Webseite haben, erfassen und analysieren Sie diese Ausgabe von einem einzigen Client:
    ```
    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. Wenn das Problem nicht behoben wird, nachdem Sie diese Schritte ausgeführt haben, sammeln Sie diese Debugs, und verwenden Sie den Support Case Manager, um eine Serviceanfrage zu öffnen.

```
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>
```

Zugehörige Informationen

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- Technischer Support und Dokumentation für Cisco Systeme

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.