Probleemoplossing voor webverificatie op een draadloze LAN-controller (WLC)

Inhoud

Inleiding

Dit document beschrijft tips om problemen met webverificatie op te lossen in een Wireless LAN Controller (WLC)-omgeving.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beheer en provisioning van draadloze access points (CAPWAP).
- Hoe u Lichtgewicht access point (LAP) en WLC kunt configureren voor basisbediening.
- Basiskennis van webverificatie en hoe webverificatie op WLC's te configureren.

Raadpleeg voor informatie over het configureren van webverificatie op WLC's het configuratievoorbeeld van de draadloze LAN-controller-webverificatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op een WLC 5500 die firmware versie 8.3.121 uitvoert.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook met deze hardware worden gebruikt:

- Cisco 5500 Series wireless controllers
- Cisco 8500 Series wireless controllers

- Cisco 2500 Series wireless controllers
- Cisco Aironet 3500 Series WLAN-controller
- Cisco Aironet 4000 Series draadloze LAN-controller
- Cisco Flex 7500 Series draadloze controllers
- Cisco draadloze servicesmodule 2 (WiSM2)

Web verificatie op WLC's

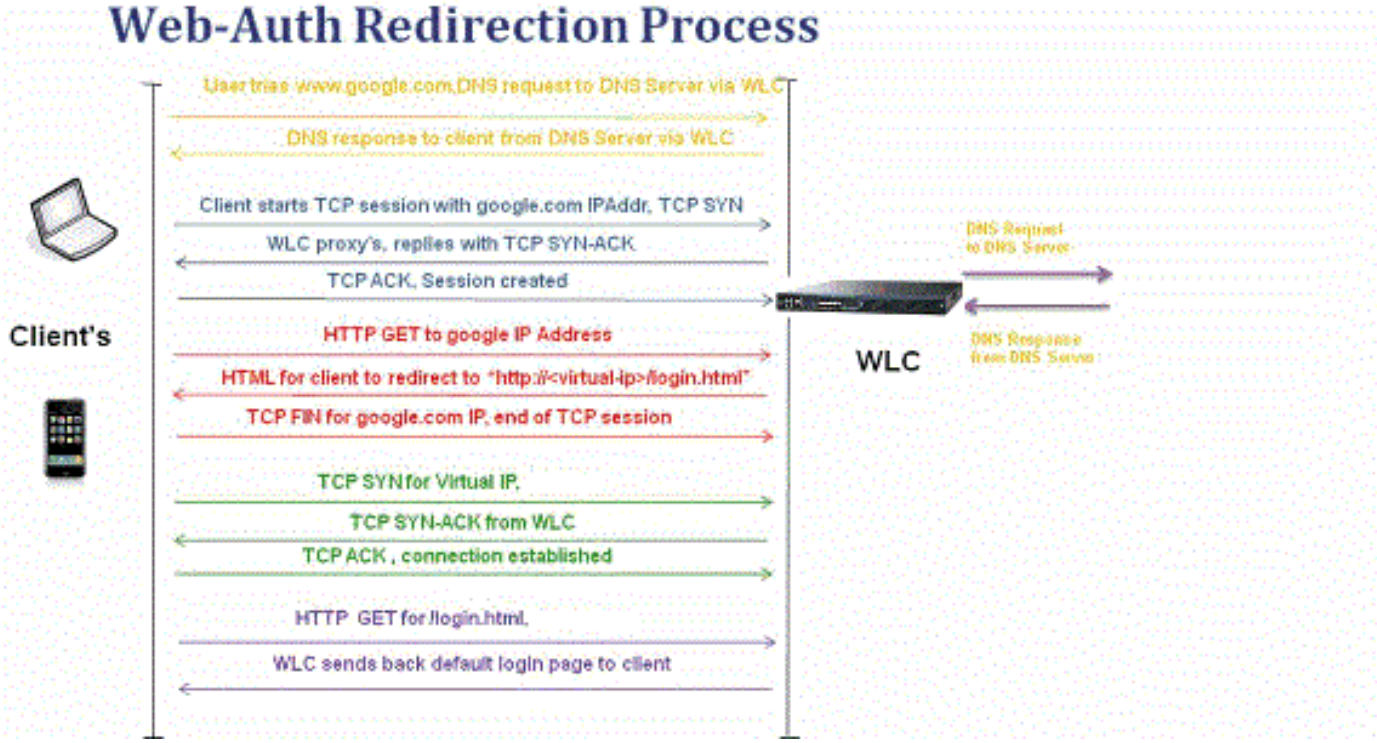
Web authenticatie is een Layer 3-beveiligingsfunctie die ervoor zorgt dat de controller geen IP-verkeer toestaat, behalve DHCP-gerelateerde pakketten/Domain Name System (DNS)-gerelateerde pakketten, van een bepaalde client totdat die client op de juiste wijze een geldige gebruikersnaam en wachtwoord heeft geleverd, met uitzondering van verkeer dat is toegestaan via een pre-auth toegangscontrolelijst (ACL). Web authenticatie is het enige beveiligingsbeleid dat de client in staat stelt om een IP-adres te krijgen voor verificatie. Het is een eenvoudige authenticatiemethode zonder de noodzaak van een supplicant of client utility. Web verificatie kan lokaal op een WLC of via een RADIUS-server worden uitgevoerd. Web authenticatie wordt meestal gebruikt door klanten die een gast-toegangsnetwerk willen implementeren.

Web authenticatie begint wanneer de controller het eerste TCP HTTP (poort 80) GET pakket van de client onderschept. Opdat de webbrowser van de client zo ver kan komen, moet de client eerst een IP-adres verkrijgen en een vertaling van de URL naar het IP-adres (DNS-resolutie) voor de webbrowser uitvoeren. Dit laat de webbrowser weten welk IP-adres om de HTTP GET te verzenden.

Wanneer webverificatie is ingesteld op het WLAN, blokkeert de controller al het verkeer (totdat het verificatieproces is voltooid) vanaf de client, behalve voor DHCP- en DNS-verkeer. Wanneer de client de eerste HTTP GET naar TCP-poort 80 verstuurt, wordt de client door de controller omgeleid naar https://192.0.2.1/login.html (als dit de virtuele IP is die is geconfigureerd) voor verwerking. Dit proces leidt uiteindelijk tot de login webpagina.

> **Opmerking**: Wanneer u een externe webserver gebruikt voor webverificatie, hebben WLC-platforms een pre-authenticatie ACL nodig voor de externe webserver.

In deze sectie wordt de omleiding van de webverificatie in detail uitgelegd.



- U opent de webbrowser en typt een URL in, bijvoorbeeld http://www.site.com. De client stuurt een DNS-verzoek voor deze URL om het IP voor de bestemming te krijgen. WLC geeft de DNS-aanvraag door aan de DNS-server en DNS-server reageert met een DNS-antwoord, dat het IP-adres van de bestemming www.site.com bevat, dat op zijn beurt wordt doorgestuurd naar de draadloze clients.
- De client probeert vervolgens een TCP verbinding te openen met het IP-adres van de bestemming. Het stuurt een TCP/SYN-pakket naar het IP-adres van www.site.com.
- De WLC heeft regels geconfigureerd voor de client en kan daarom fungeren als een proxy voor www.site.com. Het stuurt een TCP SYN-ACK pakket terug naar de client met bron als IP-adres van www.site.com. De client stuurt een TCP-ACK-pakket terug om de driewegs TCP-handdruk te voltooien en de TCP-verbinding is volledig tot stand gebracht.
- De client stuurt een HTTP GET-pakket naar www.site.com. De WLC onderschept dit pakket en verstuurt het voor omleidingsbehandeling. De HTTP applicatie gateway bereidt een HTML body voor en verstuurt het terug als het antwoord op de HTTP GET gevraagd door de client. Deze HTML maakt de client naar de standaard webpagina URL van de WLC, bijvoorbeeld http://<Virtual-Server-IP>/login.html.
- De client sluit de TCP-verbinding met het IP-adres, bijvoorbeeld www.site.com.
- De client wil nu naar http://<virtualip>/login.html gaan en probeert dus een TCP-verbinding te openen met het virtuele IP-adres van de WLC. Het verzendt een TCP SYN-pakket voor 192.0.2.1 (wat hier ons virtuele IP is) naar de WLC.
- De WLC reageert met een TCP SYN-ACK en de client stuurt een TCP-ACK terug naar de WLC om de handdruk te voltooien.
- De client stuurt een HTTP GET voor /login.html bestemd voor 192.0.2.1 om de inlogpagina aan te vragen.
- Dit verzoek is toegestaan tot de webserver van de WLC en de server reageert terug met de standaard login pagina. De client ontvangt de inlogpagina in het browservenster waar de gebruiker kan doorgaan en inloggen.

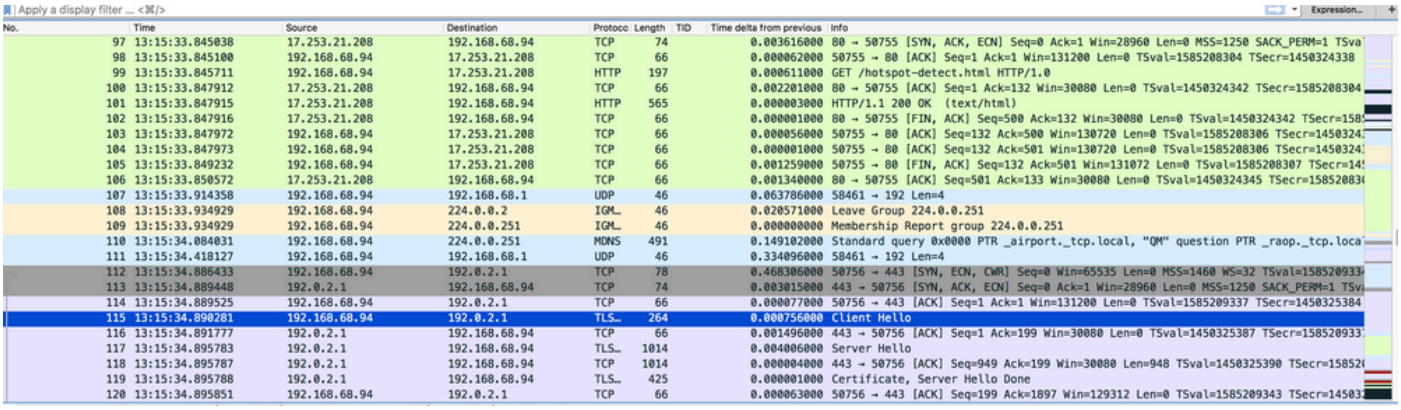
In dit voorbeeld is het IP-adres van de client 192.168.68.94. De client loste de URL naar de webserver waartoe ze toegang had, 10.1.0.13. Zoals u kunt zien, deed de client de drieweg-

handdruk om de TCP-verbinding op te starten en stuurde vervolgens een HTTP GET-pakket dat begon met pakket 96 (00 is het HTTP-pakket). Dit werd niet geactiveerd door de gebruiker, maar was het besturingssysteem geautomatiseerde portal detectie triggers (zoals we kunnen raden via de gevraagde URL). De controller onderschept de pakketten en antwoordt met code 200. Het code 200-pakket bevat een doorverwijzing naar een 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>
```

Het sluit dan de TCP verbinding door de handdruk met drie richtingen.

De client start vervolgens de HTTPS-verbinding naar de doorgestuurde URL die het verstuurt naar 192.0.2.1, wat het virtuele IP-adres is van de controller. De client moet het servercertificaat valideren of negeren om de SSL-tunnel te kunnen openen. In dit geval is het een zelfondertekend certificaat, dus de klant negeerde het. De login webpagina wordt verzonden door deze SSL-tunnel. Packet 112 begint met de transacties.



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=15852
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

U hebt de optie om de domeinnaam voor het virtuele IP adres van de WLC te configureren. Als u de domeinnaam voor het virtuele IP-adres configureert, wordt deze domeinnaam in het HTTP OK-pakket van de controller teruggestuurd naar het HTTP GET-pakket van de client. Vervolgens moet u een DNS-resolutie uitvoeren voor deze domeinnaam. Zodra het een IP-adres uit de DNS-resolutie krijgt, probeert het een TCP-sessie te openen met dat IP-adres, dat een IP-adres is dat op een virtuele interface van de controller is geconfigureerd.

Uiteindelijk wordt de webpagina door de tunnel doorgegeven aan de client en stuurt de gebruiker de gebruikersnaam/het wachtwoord terug via de SSL-tunnel (Secure Sockets Layer).

Web authenticatie wordt uitgevoerd door een van deze drie methoden:

- Gebruik een interne webpagina (standaard).
- Gebruik een aangepaste inlogpagina.
- Gebruik een inlogpagina van een externe webserver.

Opmerkingen:
- De aangepaste web authenticatie bundel heeft een limiet van maximaal 30 tekens voor bestandsnamen. Zorg ervoor dat geen bestandsnamen binnen de bundel groter zijn dan 30 tekens.

- Vanaf WLC release 7.0, als webverificatie is ingeschakeld op het WLAN en u ook CPU ACL-regels hebt, nemen de op client gebaseerde webverificatieregels altijd een hogere prioriteit zolang de client niet is geverifieerd in de staat WebAuth_Reqd. Zodra de client naar de Run-status gaat, worden de CPU ACL-regels toegepast.

- Als CPU ACL's in de WLC zijn ingeschakeld, is daarom in deze omstandigheden een acceptatieregel voor de virtuele interface IP vereist (in ELKE richting):
 - Wanneer de CPU ACL geen regel ALLE toestaan voor beide richtingen heeft.
 - Als er een voorkeursregel voor het toestaan van ALL bestaat, maar er ook een DENY-regel voor haven 443 of 80 bestaat.

- De acceptatieregel voor het virtuele IP moet zijn voor TCP-protocol en poort 80 als SecureWeb is uitgeschakeld, of poort 443 als SecureWeb is ingeschakeld. Dit is nodig om de client toegang te geven tot het virtuele IP-adres na succesvolle verificatie wanneer CPU-ACL's zijn geïnstalleerd.

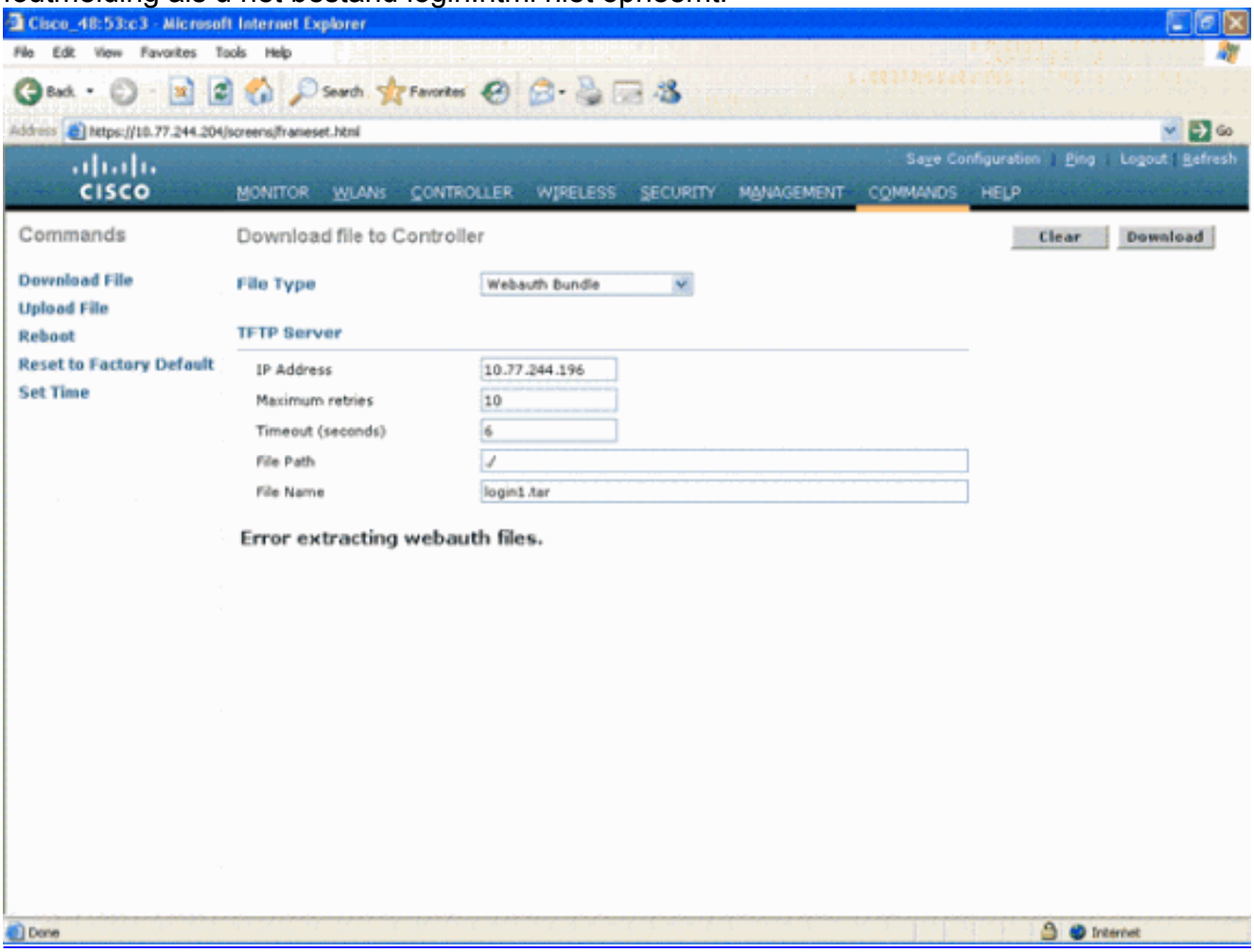
Probleemoplossing voor webverificatie

Nadat u web verificatie configureren en als de functie niet werkt zoals verwacht, voltooit u de volgende stappen:

1. Controleer of de client een IP-adres krijgt. Als dit niet het geval is, kunnen gebruikers het aanvinkvakje **DHCP Required** op het WLAN uitschakelen en de draadloze client een statisch IP-adres geven. Dit veronderstelt associatie met het access point.
2. De volgende stap in het proces is DNS resolutie van de URL in de webbrowser. Wanneer een WLAN-client verbinding maakt met een WLAN dat is geconfigureerd voor webverificatie, krijgt de client een IP-adres van de DHCP-server. De gebruiker opent een webbrowser en voert een webadres in. De client voert vervolgens de DNS-resolutie uit om het IP-adres van de website te verkrijgen. Nu, wanneer de client probeert de website te bereiken, onderschept de WLC de HTTP GET sessie van de client en leidt de gebruiker naar de web authenticatie login pagina.
3. Zorg er daarom voor dat de client in staat is DNS-resolutie uit te voeren voor de omleiding naar het werk. In Microsoft Windows, kies **Start > Uitvoeren**, voer **CMD** in om een opdrachtvenster te openen en voer een "nslookup www.cisco.com" uit om te zien of het IP-adres terugkomt. In Macs/Linux, open een terminalvenster en doe een "nslookup www.cisco.com" en kijk of het IP-adres terugkomt.Als u gelooft dat de client geen DNS-resolutie krijgt, kunt u:Voer het IP-adres van de URL in (bijvoorbeeld http://www.cisco.com is http://192.168.219.25).Probeer een willekeurig (zelfs niet-bestaand) IP-adres in te voeren dat via de draadloze adapter moet worden opgelost.Wanneer u deze URL invoert, komt die dan op de webpagina? Als ja, is het zeer waarschijnlijk een DNS probleem. Het kan ook een certificaatprobleem zijn. De controller gebruikt standaard een zelfondertekend certificaat en de meeste webbrowsers waarschuwen tegen het gebruik ervan.
4. Zorg er bij webverificatie met een aangepaste webpagina voor dat de HTML-code voor de aangepaste webpagina juist is. U kunt een voorbeeldscript voor webverificatie downloaden van Cisco-softwaredownloads. Kies bijvoorbeeld voor de 5508 controllers **Producten > Draadloos > Draadloze LAN-controller > Standalone controllers > Cisco 5500 Series draadloze LAN-controllers > Cisco 5508 draadloze LAN-controller > Software op chassis >**

Wireless LAN Controller Web Authenticatiebundel en download het bestand **webauth_bundle.zip**.Deze parameters worden toegevoegd aan de URL wanneer de internetbrowser van de gebruiker wordt omgeleid naar de aangepaste login pagina:ap_mac - Het MAC-adres van het access point waaraan de draadloze gebruiker is gekoppeld.switch_url - De URL van de controller waarop de gebruikersreferenties moeten worden geplaatst.omleiden - De URL waarnaar de gebruiker wordt omgeleid nadat de verificatie is geslaagd.statusCode - De statuscode die is teruggestuurd van de controller-webverificatieserver.WLAN - de WLAN-SSID waaraan de draadloze gebruiker is gekoppeld.Dit zijn de beschikbare statuscodes:Statuscode 1 - "U bent al ingelogd. U hoeft geen verdere actie te ondernemen."Statuscode 2 - "U bent niet ingesteld om te verifiëren via een webportal. U hoeft geen verdere actie te ondernemen."Statuscode 3 - "De opgegeven gebruikersnaam kan op dit moment niet worden gebruikt. Misschien is de gebruikersnaam al ingelogd op het systeem?"Statuscode 4 - "U bent uitgesloten."Statuscode 5 - "De ingevoerde combinatie van gebruikersnaam en wachtwoord is ongeldig. Probeer het opnieuw."

5. Alle bestanden en illustraties die moeten worden weergegeven op de aangepaste webpagina moeten worden gebundeld in een .tar bestand voordat het wordt geüpload naar de WLC. Zorg ervoor dat een van de bestanden in de .tar bundel login.html is. U ontvangt deze foutmelding als u het bestand login.html niet opneemt:



Raadpleeg de sectie Guidelines for Aangepaste Web Verification van het configuratievoorbeeld van de draadloze LAN-controller voor de webverificatie voor meer informatie over hoe u een aangepast venster voor webverificatie kunt maken.**Opmerking**: bestanden die groot zijn en bestanden met lange namen kunnen resulteren in een extractiefout. Aanbevolen wordt dat de beelden in .jpg formaat zijn.

6. Zorg ervoor dat de **Scripting** optie niet wordt geblokkeerd op de clientbrowser, aangezien de

aangepaste webpagina op de WLC in principe een HTML-script is.

7. Als u een **hostnaam** hebt geconfigureerd voor de **virtuele interface** van de WLC, zorg er dan voor dat de DNS-resolutie beschikbaar is voor de hostnaam van de virtuele interface. **Opmerking**: Navigeer naar het menu **Controller > Interfaces** van de WLC GUI om een **DNS-hostnaam** aan de virtuele interface toe te wijzen.
8. Soms blokkeert de firewall die op de clientcomputer is geïnstalleerd de inlogpagina voor webverificatie. Schakel de firewall uit voordat u probeert toegang te krijgen tot de inlogpagina. De firewall kan opnieuw worden ingeschakeld zodra de webverificatie is voltooid.
9. De topologie/oplossing firewall kan geplaatst worden tussen de client en de web-auth server, die afhankelijk is van het netwerk. Zoals voor elk geïmplementeerd netwerkontwerp/oplossing, moet de eindgebruiker ervoor zorgen dat deze poorten zijn toegestaan op de netwerkfirewall.

10. Voor webverificatie moet de client eerst koppelen aan het juiste WLAN op de WLC. Navigeer naar het menu **Monitor > Clients** op de WLC GUI om te zien of de client is gekoppeld aan de WLC. Controleer of de client een geldig IP-adres heeft.
11. Schakel de proxyinstellingen in op de clientbrowser totdat de webverificatie is voltooid.
12. De standaard webverificatiemethode is Password Authentication Protocol (PAP). Zorg ervoor dat de PAP-verificatie op de RADIUS-server is toegestaan, zodat dit werkt. Controleer de debugs en logberichten op de RADIUS-server om de status van de clientverificatie te controleren. U kunt de **debug aaa all-**opdracht op de WLC gebruiken om de debugs van de RADIUS-server te bekijken.
13. Werk het hardwarestuurprogramma op de computer bij met de laatste code van de website van de fabrikant.
14. Controleer de instellingen in de aanvrager (programma op de laptop).
15. Wanneer u de in Windows ingebouwde Windows Zero Config-applicatie gebruikt: Controleer of de gebruiker de nieuwste patches heeft geïnstalleerd.Draai debugs op de applicatie.
16. Zet op de client de APOL- (WPA+WPA2) en RASTLS-logbestanden in vanuit een opdrachtvenster. Kies **Start > Uitvoeren > CMD**:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    Als u de logbestanden wilt uitschakelen, voert u dezelfde opdracht uit maar vervangt u inschakelen door uitschakelen. Voor XP, kunnen alle logboeken in C:\Windows\tracing worden gevestigd.
17. Als u nog steeds geen inlogwebpagina hebt, verzamelt en analyseert u deze uitvoer van één 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. Als het probleem niet is opgelost nadat u deze stappen hebt voltooid, verzamelt u deze debugs en gebruikt u Support Case Manager om een serviceaanvraag te openen.
    ```
    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>
    ```

Gerelateerde informatie

- Configuratie van draadloze LAN-controller en webverificatie - voorbeeld
- Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers
- Technische ondersteuning en documentatie – Cisco Systems

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.