Begrijp webverificatie op draadloze LAN-controllers (WLC)

Inhoud

Inleiding

Dit document beschrijft de processen voor webverificatie op draadloze LAN-controllers (WLC).

Voorwaarden

Vereisten

Cisco raadt aan dat u basiskennis hebt van de WLC-configuratie.

Gebruikte componenten

De informatie in dit document is gebaseerd op alle WLC hardwaremodellen.

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.

Interne processen voor webverificatie

Web verificatie Positie als beveiligingsfunctie

Web authenticatie (WebAuth) is Layer 3-beveiliging. Het maakt gebruiksvriendelijke beveiliging mogelijk die werkt op elk station dat een browser draait.

Het kan met om het even welke pre-gedeelde zeer belangrijke (PSK) veiligheid (Layer 2 veiligheidsbeleid) worden gecombineerd.

Hoewel de combinatie van WebAuth en PSK het gebruiksvriendelijke gedeelte vermindert, heeft het het voordeel om cliëntverkeer te versleutelen.

WebAuth is een verificatiemethode zonder encryptie.

WebAuth kan niet worden geconfigureerd met 802.1x/RADIUS (Remote Verification Dial-In User Service) totdat WLC-softwarerelease 7.4 tegelijkertijd is geïnstalleerd en geconfigureerd.

Clients moeten zowel dot1x als webverificatie doorlopen. Het is bedoeld voor de toevoeging van een webportaal voor werknemers (die 802.1x gebruiken), niet gasten.

Er is geen all-in-one service set identifier (SSID) voor dot1x voor werknemers of webportal voor gasten.

Hoe WebAuth werkt

Het 802.11-verificatieproces is open, zodat u zonder problemen verificaties kunt uitvoeren en koppelen. Daarna wordt u geassocieerd, maar niet in de WLC **RUN** toestand.

Als web verificatie is ingeschakeld, blijft u binnen **WEBAUTH_REQD** waar u geen toegang hebt tot een netwerkbron.

U moet een DHCP IP-adres met het adres van de DNS-server in de opties ontvangen.

Typ een geldige URL in uw browser. De client lost de URL op via het DNS-protocol. De client stuurt vervolgens zijn HTTP-verzoek naar het IP-adres van de website.

De WLC onderschept dat verzoek en keert terug **webauth** inlogpagina, die het IP-adres van de website nabootst. Met een externe WebAuth antwoordt de WLC met een HTTP-antwoord dat uw IP-adres van de website omvat en verklaart dat de pagina is verplaatst.

De pagina werd verplaatst naar de externe webserver die door de WLC wordt gebruikt. Wanneer u wordt geverifieerd, krijgt u toegang tot alle netwerkbronnen en wordt u standaard omgeleid naar de oorspronkelijk gevraagde URL (tenzij een gedwongen omleiding is geconfigureerd op de WLC).

Samenvattend, staat WLC de client toe om de DNS op te lossen en automatisch een IP-adres te verkrijgen **WEBAUTH_REQD** toestand.

Als u een andere poort wilt bekijken in plaats van poort 80, gebruikt u **config network web-auth-port** om een omleiding op deze haven ook te creëren.

Een voorbeeld is de Access Control Server (ACS)-webinterface, die zich bevindt op poort 2002 of andere soortgelijke toepassingen.

> **Opmerking over HTTPS-omleiding**: Standaard heeft de WLC HTTPS-verkeer niet omgeleid. Dit betekent dat als u een HTTPS-adres in uw browser invoert, er niets gebeurt. U moet een HTTP-adres invoeren om te worden doorgestuurd naar de inlogpagina die in HTTPS werd geopend.
>
> In versie 8.0 en hoger kunt u omleiding van HTTPS-verkeer inschakelen met de CLI-opdracht **config network web-auth https-redirect enable.**
>
> Dit gebruikt veel bronnen voor de WLC in gevallen waarin veel HTTPS-verzoeken worden verzonden. Het is niet aan te raden om deze functie te gebruiken voor WLC versie 8.7 waar de schaalbaarheid van deze functie is verbeterd. Merk ook op dat een certificaatwaarschuwing in dit geval onvermijdelijk is. Als de client om een URL vraagt (zoals https://www.cisco.com), presenteert de WLC nog steeds zijn eigen certificaat dat is afgegeven voor het virtuele IP-adres. Dit komt nooit overeen met het URL/IP adres gevraagd door client en het certificaat wordt niet vertrouwd tenzij de client de uitzondering in hun browser afdwingt.

Indicatieve prestatiedaling van de softwarerelease WLC vóór 8.7 gemeten:

Webauth	Percentage bereikt
3 URL's - HTTP	140 / seconde
1ste URL - HTTP Tweede en derde URL's - HTTPS	20 / seconde
3 URL's - HTTPS (grote implementatie)	<1 / seconde
3 URL's - HTTPS (max. 100 clients)	10 / seconde

In deze prestatietabel worden de 3 URL's aangeduid als:

- De oorspronkelijke URL ingevoerd door de eindgebruiker
- De URL waarnaar de WLC de browser omleidt
- De definitieve indiening van de geloofsbrieven

De prestatietabel geeft de WLC-prestaties in het geval dat alle 3 URL's HTTP zijn, in het geval dat alle 3 URL's HTTPS zijn, of als de client zich van HTTP naar HTTPS beweegt (standaard).

Hoe een interne (lokale) WebAuth te laten werken met een interne pagina

Om een WLAN met een operationele dynamische interface te configureren, ontvangen de clients ook een DNS-server IP-adres via DHCP.

Voor **webauth** , wordt ingesteld, controleert of WLAN correct werkt en DNS-verzoeken kunnen worden opgelost (**nslookup**), en webpagina's kunnen worden bekeken.

Stel de webverificatie in als Layer 3-beveiligingsfuncties. Gebruikers maken in de lokale database of op een externe RADIUS-server.

Raadpleeg het configuratiedocument van de draadloze LAN-controller voor de webverificatie.

Hoe te om een Aangepaste Lokale Webex met Aangepaste Pagina te vormen

Aangepast **webauth** kan worden geconfigureerd met **redirectUrl** van de **Security** tabblad. Dit dwingt een omleiding naar een specifieke webpagina die u invoert.

Wanneer de gebruiker is geverifieerd, overschrijft deze de oorspronkelijke URL die de client heeft opgevraagd en geeft de pagina weer waarvoor de omleiding is toegewezen.

Met de aangepaste functie kunt u een aangepaste HTML-pagina gebruiken in plaats van de standaard inlogpagina. Upload uw html en image bestanden bundel naar de controller.

Ga in de uploadpagina naar **webauth bundle** in een tar-formaat. PicoZip maakt tars die compatibel zijn met de WLC.

Zie bij een voorbeeld van een WebAuth-bundel de pagina Download Software voor Wireless Controller WebAuth Bundles. Selecteer de gewenste release voor uw WLC.

Het wordt aanbevolen een bundel die bestaat aan te passen; geen nieuwe bundel maken.

Er zijn enkele beperkingen met **custom webauth** die met versies en insecten variëren.

- de grootte van het .tar-bestand (niet meer dan 5 MB)
- het aantal bestanden in de .tar
- de lengte van de bestandsnamen van de bestanden (maximaal 30 tekens)

Als het pakket niet werkt, probeer dan een eenvoudig maatpakket. Voeg bestanden en complexiteit toe om het pakket te bereiken dat de gebruiker probeerde te gebruiken. Dit helpt om het probleem te identificeren.

Om een aangepaste pagina te configureren raadpleegt u Aangepaste aanmeldpagina voor webverificatie maken, een sectie in de configuratiehandleiding voor draadloze LAN-controllers van Cisco, release 7.6.

Globale configuratietechniek negeren

Configureer met de opdracht **globale configuratie negeren** en stel een Webex-type in voor elk WLAN. Dit maakt een interne/standaard WebAuth met een aangepaste interne/standaard WebAuth voor een ander WLAN mogelijk.

Hierdoor kunnen verschillende aangepaste pagina's worden geconfigureerd voor elk WLAN.

Combineer alle pagina's in dezelfde bundel en upload ze naar de WLC.

Stel uw aangepaste pagina in met de opdracht **globale** configuratie **overschrijven** op elk WLAN en selecteer welk bestand de inlogpagina is uit alle bestanden in de bundel.

Kies een andere inlogpagina in de bundel voor elk WLAN.

Probleem met omleiding

Er is een variabele binnen de HTML-bundel die de omleiding toestaat. Plaats uw gedwongen omleiding URL daar niet.

Voor omleidingsproblemen in aangepaste Webex, raadt Cisco aan de bundel te controleren.

Als u een omleiden URL met **+=**in de WLC GUI invoert, kan dit overschrijven *of* toevoegen aan de URL die binnen de bundel is gedefinieerd.

In de WLC GUI, bijvoorbeeld, is de **redirectURL** het veld wordt ingesteld op www.cisco.com; in de bundel is echter te zien: **redirectURL+=** "(URL van de website)". Met **+=** worden gebruikers omgeleid naar een ongeldige URL.

Hoe een externe (lokale) webverificatie te laten werken met een externe pagina

Het gebruik van een externe WebAuth-server is slechts een externe opslagplaats voor de inlogpagina. De gebruikersreferenties worden nog steeds geverifieerd door de WLC. De externe webserver staat alleen een speciale of andere inlogpagina toe.

Stappen uitgevoerd voor een externe Webex:

1. De client (eindgebruiker) opent een webbrowser en voert een URL in.

2. Als de client niet is geverifieerd en externe webverificatie wordt gebruikt, wordt de gebruiker door de WLC omgeleid naar de externe webserver URL. De WLC stuurt een HTTP-omleiding naar de client met het geïmiteerde IP-adres en wijst naar het IP-adres van de externe server. De externe URL voor webverificatie wordt toegevoegd met parameters zoals de **AP_Mac_Address**,het **client_url** (client-URL-adres) en **action_URL** nodig om contact op te nemen met de switch-webserver.

3. De externe webserver URL stuurt de gebruiker naar een inlogpagina. De gebruiker kan een toegangscontrolelijst (ACL) voor verificatie gebruiken om toegang te krijgen tot de server.

4. De inlogpagina verstuurt de gebruikersreferenties terug naar de **action_URL**, zoals http://192.0.2.1/login.html, van de WLC webserver. Dit wordt geleverd als invoerparameter voor de omleiding URL, waar 192.0.2.1 het virtuele interfaceadres op de switch is.

5. De WLC webserver dient de gebruikersnaam en het wachtwoord in voor verificatie.

6. De WLC initieert het RADIUS-serververzoek of gebruikt de lokale database op de WLC, en

verifieert vervolgens de gebruiker.

7. Als de verificatie succesvol is, stuurt de WLC-webserver de gebruiker door naar de geconfigureerde doorverwijzing-URL of naar de URL die de client is ingevoerd.

8. Als de authenticatie mislukt, dan zal de WLC-webserver de gebruiker terugleiden naar de gebruikerslogin URL.

   Opmerking : we gebruiken 192.0.2.1 als voorbeeld van virtuele ip in dit document. Het 192.0.2.x-bereik is aangeraden voor virtueel IP omdat het niet routeerbaar is. Oudere documentatie verwijst mogelijk naar "1.1.1.x" of is nog steeds wat in uw WLC is geconfigureerd, aangezien dit de standaardinstelling was. Houd er echter rekening mee dat dit IP nu een geldig routable IP-adres is en daarom het 192.0.2.x-subnetnummer wordt geadviseerd.

Als de toegangspunten (AP's) zich in de FlexConnect-modus bevinden, selecteert u een **preauth** ACL is irrelevant. Flex ACL's kunnen worden gebruikt om toegang tot de webserver mogelijk te maken voor clients die niet zijn geverifieerd.

Raadpleeg het configuratievoorbeeld van de externe webverificatie met draadloze LAN-controllers.

Web Passthrough

Web Passthrough is een variatie van de interne webverificatie. Het toont een pagina met een waarschuwing of een waarschuwingsverklaring, maar vraagt niet om referenties.

De gebruiker klikt dan op **OK**. Laat e-mailinput toe en de gebruiker kan hun e-mailadres invoeren dat hun gebruikersnaam wordt.

Wanneer de gebruiker is verbonden, controleert u de lijst met actieve clients en controleert u of de gebruiker is vermeld met het e-mailadres dat hij als gebruikersnaam heeft ingevoerd.

Raadpleeg voor meer informatie het voorbeeld van de configuratie van de draadloze LAN-controller 5760/3850 Web Passthrough.

Voorwaardelijke omleiding van web

Als u een voorwaardelijke web redirect inschakelt, wordt de gebruiker voorwaardelijk omgeleid naar een bepaalde webpagina nadat de 802.1x-verificatie met succes is voltooid.

U kunt de omleidingspagina en de voorwaarden waaronder de omleiding op uw RADIUS-server plaatsvindt, specificeren.

De voorwaarden kunnen het wachtwoord omvatten wanneer het de verloopdatum bereikt of wanneer de gebruiker een rekening voor voortgezet gebruik/toegang moet betalen.

Als de RADIUS-server het Cisco AV-paar retourneert **url-redirect**Vervolgens wordt de gebruiker doorgestuurd naar de opgegeven URL wanneer een browser wordt geopend.

Als de server ook het Cisco AV-paar retourneert **url-redirect-acl**Vervolgens wordt de opgegeven ACL geïnstalleerd als een pre-verificatie ACL voor deze client.

De client wordt op dit punt niet als volledig geautoriseerd beschouwd en kan alleen verkeer doorgeven dat is toegestaan door de ACL voor verificatie. Nadat de client een bepaalde bewerking op de opgegeven URL heeft voltooid (bijvoorbeeld een wachtwoordwijziging of betaling van de factuur), moet de client opnieuw worden geverifieerd.

Wanneer de RADIUS-server geen **url-redirect**, wordt de cliënt geacht over een volledige vergunning te beschikken en over een vergunning te beschikken voor het doorgeven van verkeer.

> **Opmerking:** De voorwaardelijke web redirect functie is alleen beschikbaar voor WLAN's die zijn geconfigureerd voor 802.1x of WPA+WPA2 Layer 2-beveiliging.

Na configuratie van de RADIUS-server moet u het voorwaardelijke web configureren en op de controller omleiden met de controller GUI of CLI. Raadpleeg deze stapsgewijze handleidingen: Web Redirect (GUI) configureren en Web Redirect (CLI) configureren.

Webomleiding spraakpagina

Als u splash pagina web redirect inschakelt, wordt de gebruiker omgeleid naar een bepaalde webpagina nadat de 802.1x-verificatie met succes is voltooid. Nadat de omleiding is uitgevoerd, heeft de gebruiker volledige toegang tot het netwerk.

U kunt de omleidingspagina op uw RADIUS-server specificeren. Als de RADIUS-server het Cisco AV-paar retourneert **url-redirect**Vervolgens wordt de gebruiker doorgestuurd naar de opgegeven URL wanneer een browser wordt geopend.

De client wordt op dit punt als volledig geautoriseerd beschouwd en mag verkeer doorgeven, zelfs als de RADIUS-server geen **url-redirect**.

> **Opmerking:** De functie voor omleiding van spatpagina is alleen beschikbaar voor WLAN's die zijn geconfigureerd voor 802.1x of WPA+WPA2 Layer 2-beveiliging.

Nadat de RADIUS-server is geconfigureerd, configureer dan het splash-pagina-web opnieuw op de controller met de controller GUI of CLI.

WebAuth op MAC Filter fout

Een WebAuth op MAC Filter FaFailure vereist dat u MAC-filters in Layer 2 security menu configureren.

Als gebruikers met succes worden gevalideerd met hun MAC-adressen, gaan ze direct naar de **run** toestand.

Zo niet, dan gaan zij naar de **WEBAUTH_REQD** status en de normale webverificatie vindt plaats.

> **Opmerking:** Dit wordt niet ondersteund met web passthrough.Voor meer informatie, volg de activiteit op de enhanceverzoek Cisco bug ID CSCtw73512

Centrale webverificatie

Central Web Verification verwijst naar een scenario waarbij de WLC niet langer als host fungeert. De client wordt rechtstreeks naar de ISE webportal gestuurd en gaat niet door 192.0.2.1 op de WLC. De inlogpagina en de gehele portal worden geëxternaliseerd.

Central Web Verification vindt plaats wanneer RADIUS Network Admission Control (NAC) is ingeschakeld in de geavanceerde instellingen van de WLAN- en MAC-filters.

De WLC stuurt een RADIUS-verificatie (meestal voor het MAC-filter) naar ISE, die met de **redirect-url** paar attribuutwaarde (AV).

De gebruiker wordt vervolgens ingeschakeld **POSTURE_REQD** staat totdat ISE de vergunning verleent met een verzoek tot wijziging van de vergunning. Hetzelfde scenario gebeurt in Posture of Central WebAuth.

Central WebAuth is niet compatibel met WPA-Enterprise/802.1x omdat het gastportaal geen sessiesleutels voor versleuteling kan retourneren, zoals bij EAP (Extensible Verification Protocol).

Externe gebruikersverificatie (RADIUS)

Externe Gebruikersverificatie (RADIUS) is alleen geldig voor Local WebAuth wanneer WLC de referenties behandelt of wanneer een Layer 3-webbeleid is ingeschakeld. Verifieer gebruikers lokaal of op de WLC of extern via RADIUS.

Er is een volgorde waarin de WLC de referenties van de gebruiker controleert.

1. In ieder geval kijkt het eerst in zijn eigen database.
2. Als het de gebruikers daar niet vindt, gaat het naar de server van de RADIUS die in de gast WLAN wordt gevormd (als er één wordt gevormd).
3. Vervolgens wordt in de algemene RADIUS-serverlijst vergeleken met de RADIUS-servers waarop **network user** gecontroleerd.

Dit derde punt beantwoordt de vraag van hen die geen RADIUS voor dat WLAN vormen, maar merk op dat het nog steeds controleert tegen de RADIUS wanneer de gebruiker niet op de controller wordt gevonden.

Dit komt doordat **network user** wordt gecontroleerd aan de hand van uw RADIUS-servers in de algemene lijst.

WLC kan gebruikers authenticeren naar RADIUS-server met Password Authentication Protocol (PAP), Challenge Handshake Verification Protocol (CHAP) of EAP-MD5 (Message Digest5).

Dit is een globale parameter en is configureerbaar van GUI of CLI:

Van GUI: navigeren naar **Controller > Web RADIUS Authentication**

Van CLI: voer in **config custom-web RADIUSauth**

> Opmerking:De NAC-gastserver gebruikt alleen PAP.

Hoe een bekabeld gast WLAN instellen

Een Wireless Guest WLAN-configuratie is vergelijkbaar met een draadloze gastconfiguratie. Het kan worden geconfigureerd met een of twee controllers (alleen als een auto-anker is).

Kies een VLAN als het VLAN voor bekabelde gastgebruikers, bijvoorbeeld op VLAN 50. Wanneer een bekabelde gast toegang tot internet wil, steek de laptop in een poort op een switch die voor VLAN 50 is geconfigureerd.

Dit VLAN 50 moet worden toegestaan en op het pad aanwezig zijn via de WLC-trunkpoort.

In een geval van twee WLCs (één anker en één buitenlands), moet dit bekabelde gast VLAN leiden tot de buitenlandse WLC (genoemd WLC1) en niet tot het anker.

WLC1 zorgt dan voor de verkeerstunnel naar de DMZ WLC (het anker, genaamd WLC2), die het verkeer in het routed netwerk vrijgeeft.

Hier zijn de vijf stappen om bekabelde gasttoegang te configureren:

1. Configureer een dynamische interface (VLAN) voor bekabelde gastgebruikerstoegang.

   Op WLC1 maakt u een dynamische interface VLAN50. In de **interface configuration** pagina, controleer **Guest LAN** doos. Vervolgens worden velden zoals **IP address** en **gateway** verdwijnen. WLC moet erkennen dat het verkeer van VLAN 50 wordt gerouteerd. Deze cliënten zijn getelegrafeerde gasten.

2. Maak een bekabeld LAN voor gastentoegang.

   Op een controller wordt een interface gebruikt wanneer deze aan een WLAN is gekoppeld. Maak vervolgens een WLAN aan op uw belangrijkste kantoorcontrollers. Navigeer naar **WLANs** en klik op **New**. In **WLAN Type**, kiezen **Guest LAN**.

   Voer in Profielnaam en WLAN-SSID een naam in die dit WLAN identificeert. Deze namen kunnen verschillend zijn, maar kunnen geen ruimten bevatten. De term WLAN wordt gebruikt, maar dit netwerkprofiel is niet gekoppeld aan het profiel voor een draadloos netwerk.

   Het **General** tab biedt twee vervolgkeuzelijsten: **Ingress** en **Egress**. Ingress is het VLAN waar gebruikers vandaan komen (VLAN 50); Uitgang is het VLAN waarnaar u hen verzendt.

   Voor **Ingress**, kiezen **VLAN50**.

   Voor **Egress**Maar het is anders. Als u slechts één controller hebt, maakt u een andere dynamische interface, een **standard** één dit keer (niet een gast LAN), en verzend bekabelde gebruikers naar deze interface. In dit geval, stuur ze naar de DMZ controller. Daarom **Egress** interface kiest u de **Management Interface**.

   Het **Security** De modus voor dit gastLAN "WLAN" is WebAuth, wat acceptabel is. Klik **Ok** om te

valideren.

3. **Configureer de buitenlandse controller (hoofdkantoor).**

   Van de **WLAN list**klikt u op **Mobility Anchor** aan het eind van het **Guest LAN** lijn, en kies uw DMZ controller. Er wordt aangenomen dat beide controllers elkaar herkennen. Zo niet, ga naar **Controller** > **Mobility Management** > **Mobility group**, en voeg **DMZWLC** op WLC1 toe. Voeg vervolgens **WLC1** op DMZ toe. Beide luchtverkeersleiders mogen niet tot dezelfde mobiliteitsgroep behoren. Anders zijn de basisveiligheidsregels overtreden.

4. **Configureer de ankercontroller (de DMZ-controller).**

   De belangrijkste kantoorcontroller is klaar. Bereid nu uw DMZ controller voor. Open een webbrowsersessie voor uw DMZ-controller en navigeer naar **WLAN's**. Maak een nieuw WLAN. In **WLAN Type**, kiezen **Guest LAN**.

   In **Profile Name** en **WLAN SSID**Voer een naam in die dit WLAN identificeert. Gebruik dezelfde waarden als die ingevoerd zijn op de hoofdkantoorcontroller.

   Het **Ingress** De interface is **None**. Dit is niet van belang omdat het verkeer wordt ontvangen via de Ethernet over IP (EoIP)-tunnel. Het is niet nodig om een Ingress interface te specificeren.

   Het **Egress** De interface is waar de cliënten moeten worden verzonden. De **DMZ VLAN** is VLAN 9. Maak een standaard dynamische interface voor VLAN 9 op uw DMZWLC en kies vervolgens **VLAN 9** als de uitgaande interface.

   Configureer het einde van de Mobility Anchor-tunnel. Kies in de **WLAN-lijst** **Mobility Anchor for Guest LAN**. Verzend het verkeer naar de lokale controller, **DMZWLC**. Beide eindjes zijn nu klaar.

5. **Verfijn het gastnetwerk.**

   U kunt de WLAN-instellingen aan beide uiteinden ook verfijnen. De instellingen moeten aan beide uiteinden identiek zijn. Als u bijvoorbeeld op de **WLAN Advanced** tabblad, **Allow AAA override** voor WLC1, controleer dezelfde doos op DMZWLC. Als er verschillen zijn in het WLAN aan beide zijden, breekt de tunnel. DMZWLC weigert het verkeer; u kunt zien wanneer u **run debug mobility**.

   Houd in gedachten dat alle waarden daadwerkelijk uit DMZWLC worden verkregen: IP-adressen, VLAN-waarden enzovoort. Configureer de WLC1-kant identiek, zodat het de aanvraag doorgeeft aan de WLCDMZ.

Certificaten voor de aanmeldpagina

Deze sectie biedt de processen om uw eigen certificaat op de WebAuth pagina te zetten, of om de 192.0.2.1 WebAuth URL te verbergen en een genoemde URL weer te geven.

Upload een certificaat voor de webverificatie van de controller

Via de GUI (**WebAuth > Certificate**) of CLI (overdrachtstype) **webauthcert**) u kunt een certificaat uploaden op de controller.

Of het nu gaat om een certificaat dat is gemaakt met uw certificeringsinstantie (CA) of een officiële certificaat van derden, het moet in .pem-formaat zijn.

Voordat u verstuurt, moet u ook de sleutel van het certificaat invoeren.

Na het uploaden moet de computer opnieuw worden opgestart om het certificaat te kunnen installeren. Nadat u de computer hebt opgestart, gaat u naar de pagina met het Webex-certificaat in de GUI om de gegevens te vinden van het certificaat dat u hebt geüpload (geldigheid enzovoort).

Het belangrijke veld is de algemene naam (CN), de naam die aan het certificaat wordt toegekend. Dit veld wordt in dit document besproken onder de sectie "Certificaatautoriteit en andere certificaten op de controller".

Nadat u de gegevens van het certificaat opnieuw hebt opgestart en geverifieerd, wordt u op de inlogpagina van WebAuth met het nieuwe controllercertificaat gepresenteerd. Er kunnen echter twee situaties zijn.

1. Als uw certificaat is afgegeven door een van de weinige hoofdbron CA's die elke computer vertrouwt, dan is het oké. Een voorbeeld is VeriSign, maar u wordt gewoonlijk ondertekend door een Verisign sub-CA en niet de wortel CA. U kunt uw browser certificaatwinkel inchecken als u de daar vermelde CA als vertrouwd ziet.

2. Als u uw certificaat van een kleiner bedrijf/CA, alle computers vertrouwen hen niet. Verstrek het bedrijf/CA-certificaat ook aan de klant, en een van de basis-CA's geeft dat certificaat af. Uiteindelijk hebt u een keten zoals "Certificaat is afgegeven door CA x > CA x certificaat is afgegeven door CA y > CA y certificaat is afgegeven door deze vertrouwde root CA". Het einddoel is een CA te bereiken die de klant vertrouwt.

Certificaatautoriteit en andere certificaten op de controller

Om te worden bevrijd van de waarschuwing "dit certificaat wordt niet vertrouwd", voer het certificaat van de CA die het certificaat van de controller heeft afgegeven in op de controller.

Vervolgens presenteert de controller beide certificaten (het controller certificaat en het CA certificaat). Het CA-certificaat moet een vertrouwde CA zijn of de bronnen hebben om de CA te verifiëren. U kunt daadwerkelijk een keten CA-certificaten bouwen die leiden tot een vertrouwde CA op de top.

Plaats de gehele keten in hetzelfde bestand. Het bestand bevat dan inhoud zoals dit voorbeeld:

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

Hoe zorgt u ervoor dat het certificaat overeenkomt met de URL

De WebAuth URL is ingesteld op 192.0.2.1 om te authenticeren en het certificaat wordt afgegeven (dit is het CN veld van het WLC certificaat).

Als u de WebAuth URL bijvoorbeeld wilt wijzigen in 'myWLC.com', gaat u naar de **virtual interface configuration** (de interface 192.0.2.1) en hier kunt u een **virtual DNS hostname**, zoals myWLC.com.

Dit vervangt de 192.0.2.1 in uw URL-balk. Deze naam moet ook oplosbaar zijn. Het snuffelspoor toont hoe het allemaal werkt, maar wanneer WLC de login pagina verstuurt, toont WLC het myWLC.com adres, en de client lost deze naam op met hun DNS.

Deze naam moet oplossen als 192.0.2.1. Dit betekent dat als u ook een naam gebruikt voor het beheer van de WLC, een andere naam gebruikt voor WebAuth.

Als u myWLC.com in kaart gebracht aan het WLC beheer IP adres gebruikt, moet u een andere naam voor WebAuth, zoals myWLCwebauth.com gebruiken.

Problemen met certificaten oplossen

In deze sectie wordt uitgelegd hoe en wat u moet controleren om problemen met certificaten op te lossen.

Hoe

Download OpenSSL (voor Windows, zoek naar OpenSSL Win32) en installeer het. Zonder enige configuratie, kunt u gaan in de bin directory en proberen **openssl s_client –connect (your web auth URL):443**,

Als deze URL de URL is waar uw WebAuth-pagina aan uw DNS is gekoppeld, raadpleegt u "Wat te controleren" in de volgende sectie van dit document.

Als uw certificaten een private CA gebruiken, plaats het Root CA-certificaat in een directory op een lokale machine en gebruik de openssl-optie **-CApath**. Als je een tussenliggende CA hebt, zet het dan ook in dezelfde directory.

Om algemene informatie over het certificaat te verkrijgen en te controleren, gebruikt u:

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

Het is ook handig om certificaten te converteren met het gebruik van openssl:

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

Wat te controleren

U kunt zien welke certificaten naar de client worden verzonden wanneer deze verbinding maakt. Lees het apparaatcertificaat — de CN moet de URL zijn waar de webpagina bereikbaar is.

Lees de "uitgegeven door" regel van het apparaatcertificaat. Dit moet overeenkomen met de GN van het tweede certificaat. Dit tweede certificaat, "afgegeven door", moet overeenkomen met de GN van het volgende certificaat, enz. Anders maakt het geen echte keten.

In de hier getoonde OpenSSL-uitvoer ziet u dat **openssl** kan het apparaatcertificaat niet verifiëren omdat het "afgegeven door" niet overeenkomt met de naam van het CA-certificaat dat is verstrekt.

SSL-uitgang

```
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)
---
```

Een andere mogelijke kwestie is dat het certificaat niet kan worden geüpload naar de controller. In deze situatie is er geen sprake van geldigheid, CA, enzovoort.

Om dit te verifiëren, controleer de Trivial File Transfer Protocol (TFTP) connectiviteit en probeer een configuratiebestand over te brengen. Als u de **debug transfer all enable** bevel, merk op dat het probleem de installatie van het certificaat is.

Dit kan te wijten zijn aan de verkeerde sleutel gebruikt met het certificaat. Het kan ook zijn dat het certificaat in een verkeerd formaat is of is beschadigd.

Cisco raadt u aan de certificaatinhoud te vergelijken met een bekend, geldig certificaat. U kunt dan zien of een **LocalkeyID** attribuut toont alle 0s (reeds gebeurd). Zo ja, dan moet het certificaat opnieuw worden omgezet.

Er zijn twee commando's met OpenSSL waarmee je van .pem naar .p12 kunt terugkeren en vervolgens een .pem opnieuw kunt uitgeven met de sleutel van je keuze.

Als u een .pem-document met een certificaat gevolgd door een sleutel hebt ontvangen, kopieert/plakt u het belangrijkste onderdeel: **----BEGIN KEY ---- until ------- END KEY ------** van de .pem naar "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? U wordt gevraagd om een toets; voer in **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** Dit resulteert in een operationele .pem met het wachtwoord **check123**.

Andere situaties voor probleemoplossing

Hoewel **mobiliteitshanker** niet in dit document is besproken, als u in een **verankerde** gastsituatie bent, zorg ervoor dat de mobiliteitsuitwisseling correct plaatsvindt en dat u de client op het anker ziet aankomen.

Voor eventuele verdere problemen met de webautorisatie moet probleemoplossing worden uitgevoerd op het anker.

Hier zijn enkele veelvoorkomende problemen die u kunt oplossen:

- **Gebruikers kunnen niet koppelen aan het WLAN**.

  Dit heeft niets te maken met WebAuth. Controleer de clientconfiguratie, de beveiligingsinstellingen op het WLAN, indien ingeschakeld, en of radio's actief en actief zijn, enzovoort.

- **Gebruikers verkrijgen geen IP-adres**.

  In een gast anker situatie, is dit meestal omdat het buitenlands en anker niet precies de zelfde manier werd gevormd. Controleer anders de DHCP-configuratie, connectiviteit, enzovoort.
- Controleer of andere WLAN's dezelfde DHCP-server zonder probleem kunnen gebruiken. Dit heeft niets te maken met WebAuth.

- **Gebruiker wordt niet doorgestuurd naar de inlogpagina**.

  Dit is het meest voorkomende symptoom, maar is preciezer. Er zijn twee mogelijke scenario's.

  De gebruiker wordt niet omgeleid (gebruiker voert een URL in en bereikt nooit de WebAuth pagina). Controleer voor deze situatie:

  dat een geldige DNS-server via DHCP aan de client is toegewezen (**ipconfig /all**),

  dat DNS van de cliënt bereikbaar is (**nslookup (website URL**),

dat de gebruiker een geldige URL heeft ingevoerd om doorgestuurd te worden,

dat de gebruiker ging op een HTTP URL op poort 80 (bijvoorbeeld, om een ACS met http://localhost:2002 te bereiken wordt u niet omgeleid sinds u op poort 2002 in plaats van 80 hebt verzonden).

De gebruiker wordt correct omgeleid naar 192.0.2.1, maar de pagina zelf wordt niet weergegeven.

Deze situatie is zeer waarschijnlijk of een probleem WLC (bug) of een client-side probleem. Het kan zijn dat de client een firewall of software of beleidsblokkering heeft. Het kan ook zijn dat ze een proxy hebben geconfigureerd in hun webbrowser.

Aanbeveling: Volg de sniffer op de client-pc. Er is geen behoefte aan speciale draadloze software, alleen Wireshark, die draait op de draadloze adapter en u laat zien of de WLC antwoordt en probeert om te leiden. Je hebt twee mogelijkheden: of er is geen reactie van WLC, of er is iets mis met de SSL handdruk voor de WebAuth pagina. Voor SSL handdruk probleem, kunt u controleren of de gebruikersbrowser SSLv3 toestaat (sommigen staan slechts SSLv2 toe), en als het te agressief op certificaatverificatie is.

Het is een veel voorkomende stap om handmatig http://192.0.2.1 in te voeren om te controleren of de webpagina zonder DNS verschijnt. Je kunt eigenlijk http://10.0.0.0 typen en hetzelfde effect krijgen. De WLC stuurt elk IP-adres dat u invoert om. Daarom, als u http://192.0.2.1 invoert, maakt het u niet werken rond de webomleiding. Als u https://192.0.2.1(beveiligd) invoert, werkt dit niet omdat WLC het HTTPS-verkeer niet omleidt (standaard is dit mogelijk in Versie 8.0 en hoger). De beste manier om de pagina direct te laden zonder een redirect is door https://192.0.2.1/login.html in te voeren.

- **Gebruikers kunnen niet verifiëren**.

  Zie het gedeelte van dit document waarin de verificatie wordt besproken. Controleer de referenties lokaal op de RADIUS.

- **Gebruikers kunnen met succes authenticeren via WebAuth, maar ze hebben daarna geen internettoegang**.

  U kunt WebAuth verwijderen uit de beveiliging van het WLAN, en dan hebt u een open WLAN. Je kan dan proberen om toegang te krijgen tot het web, de DNS enzovoort. Als u daar ook problemen ondervindt, verwijder dan de instellingen van WebAuth helemaal en controleer de configuratie van uw interfaces.

Zie voor meer informatie: Webverificatie voor probleemoplossing op een draadloze LAN-controller (WLC).

HTTP-proxyserver en hoe het werkt

U kunt een HTTP proxy server gebruiken. Als u de client nodig hebt om een uitzondering toe te

voegen in zijn browser dat 192.0.2.1 niet door de proxyserver moet gaan, kunt u de WLC laten luisteren naar HTTP-verkeer op de poort van de proxyserver (meestal 8080).

Om dit scenario te begrijpen, moet je weten wat een HTTP proxy doet. Het is iets dat u aan de clientzijde (IP-adres en poort) in de browser vormt.

Het gebruikelijke scenario wanneer een gebruiker een website bezoekt is om de naam aan IP met DNS op te lossen, en dan vraagt het de webpagina aan de webserver. Het proces verzendt altijd het HTTP-verzoek voor de pagina naar de proxy.

De proxy verwerkt de DNS, indien nodig, en doorstuurt naar de webserver (als de pagina nog niet op de proxy is gecached). De discussie gaat alleen over client-to-proxy. Of de proxy de echte webpagina krijgt of niet, is niet relevant voor de klant.

Hier is het web authenticatie proces:

- Gebruikerstypen in een URL.
- De client-pc verstuurt naar de proxyserver.
- WLC-onderscheppingen en -imitaties Proxyserver IP; het antwoordt op de PC met een doorverwijzing naar 192.0.2.1

In dit stadium, als de PC niet is geconfigureerd voor het, vraagt het om de 192.0.2.1 WebAuth pagina naar de proxy zodat het niet werkt. De PC moet een uitzondering maken voor 192.0.2.1; dan stuurt het een HTTP-verzoek naar 192.0.2.1 en gaat verder met WebAuth.

Na authenticatie gaan alle communicaties weer door een proxy. Een uitzonderingsconfiguratie is meestal in de browser dicht bij de configuratie van de proxyserver. U ziet dan het bericht: "Gebruik geen proxy voor die IP-adressen".

Met WLC release 7.0 en hoger is deze functie **webauth proxy redirect** kan worden ingeschakeld in de globale WLC-configuratieopties.

Als deze optie is ingeschakeld, controleert de WLC of de clients zijn geconfigureerd om handmatig een proxy te gebruiken. In dat geval sturen ze de client door naar een pagina die laat zien hoe ze hun proxyinstellingen kunnen aanpassen om alles te laten werken.

De WebAuth proxy redirect kan worden geconfigureerd om te werken aan een verscheidenheid aan poorten en is compatibel met Central Web Verification.

Raadpleeg bij een voorbeeld van een omleiding van een WebAuth-proxy de Web Verification Proxy op een configuratievoorbeeld van een draadloze LAN-controller.

Web verificatie op HTTP in plaats van HTTPS

U kunt inloggen op webverificatie op HTTP in plaats van op HTTPS. Als u inlogt op HTTP, ontvangt u geen certificaatwaarschuwingen.

Voor eerder dan WLC release 7.2 code, moet u HTTPS-beheer van WLC uitschakelen en HTTP-beheer verlaten. Dit staat echter alleen het webbeheer van de WLC toe via HTTP.

Voor de WLC release 7.2-code gebruikt u de **config network web-auth secureweb disable** opdracht om uit te schakelen. Dit schakelt alleen HTTPS uit voor webverificatie en niet voor het beheer. Merk op dat dit een reboot van de controller vereist!

Op WLC release 7.3 en latere code kunt u HTTPS voor Webex alleen via GUI en CLI in- en uitschakelen.

Gerelateerde informatie

- Configuratie van draadloze LAN-controller en webverificatie - voorbeeld
- Software downloaden voor draadloze controller en webautorisatiebundels
- Een aangepaste aanmeldpagina voor webverificatie maken
- Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers
- Configuratie-voorbeeld van draadloze LAN-controller 5760/3850 Web Passthrough
- Web Redirect configureren (GUI)
- Web Redirect (CLI) configureren
- Webverificatie voor probleemoplossing op een draadloze LAN-controller (WLC)
- Configuratievoorbeeld van webverificatie op een draadloze LAN-controller
- Requests for Comments (RFC's)
- 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.