Informazioni sull'autenticazione Web sui controller WLC

Sommario

Introduzione

Questo documento descrive i processi di autenticazione Web sui controller WLC.

Prerequisiti

Requisiti

Cisco consiglia di avere una conoscenza base della configurazione WLC.

Componenti usati

Le informazioni di questo documento si basano su tutti i modelli hardware WLC.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Processi interni di autenticazione Web

Posizione di autenticazione Web come funzionalità di sicurezza

L'autenticazione Web (WebAuth) è una protezione di livello 3. Offre una sicurezza intuitiva che funziona su qualsiasi stazione che esegue un browser.

Può essere combinato con qualsiasi protezione con chiave già condivisa (PSK) (policy di sicurezza di livello 2).

Sebbene la combinazione di WebAuth e PSK riduca la parte di facile utilizzo, ha il vantaggio di crittografare il traffico dei client.

WebAuth è un metodo di autenticazione senza crittografia.

WebAuth non può essere configurato con 802.1x/RADIUS (Remote Authentication Dial-In User Service) finché il software WLC versione 7.4 non viene installato e configurato contemporaneamente.

I client devono eseguire sia l'autenticazione dot1x che l'autenticazione Web. È stato progettato per l'aggiunta di un portale Web per i dipendenti (che utilizzano 802.1x), non per gli ospiti.

Non esiste un SSID (Service Set Identifier) all-in-one per il dot1x per i dipendenti o un portale Web per gli ospiti.

Funzionamento di WebAuth

Il processo di autenticazione 802.11 è aperto, quindi è possibile eseguire l'autenticazione e l'associazione senza problemi. In seguito, l'utente viene associato, ma non nel WLC **RUN** state.

Se l'autenticazione Web è attivata, l'utente rimane **WEBAUTH_REQD** in cui non è possibile accedere ad alcuna risorsa di rete.

Ènecessario ricevere un indirizzo IP DHCP con l'indirizzo del server DNS nelle opzioni.

Digitare un URL valido nel browser. Il client risolve l'URL tramite il protocollo DNS. Il client invia quindi la richiesta HTTP all'indirizzo IP del sito Web.

Il WLC intercetta tale richiesta e restituisce il **webauth** che imita l'indirizzo IP del sito Web. Con un WebAuth esterno, il WLC risponde con una risposta HTTP che include l'indirizzo IP del sito Web e

indica che la pagina è stata spostata.

La pagina è stata spostata nel server Web esterno utilizzato dal WLC. Una volta autenticati, si ottiene l'accesso a tutte le risorse di rete e si viene reindirizzati all'URL richiesto in origine per impostazione predefinita (a meno che non sia stato configurato un reindirizzamento forzato sul WLC).

In sintesi, il WLC consente al client di risolvere il DNS e ottenere automaticamente un indirizzo IP in **WEBAUTH_REQD** state.

Per controllare un'altra porta anziché la porta 80, utilizzare **config network web-auth-port** per creare un reindirizzamento anche su questa porta.

Un esempio è l'interfaccia Web di Access Control Server (ACS), che si trova sulla porta 2002 o in altre applicazioni simili.

> **Nota sul reindirizzamento HTTPS**: Per impostazione predefinita, il WLC non reindirizza il traffico HTTPS. Ciò significa che se si digita un indirizzo HTTPS nel browser, non accade nulla. È necessario digitare un indirizzo HTTP per essere reindirizzati alla pagina di accesso fornita in HTTPS.
>
> Nella versione 8.0 e successive, è possibile abilitare il reindirizzamento del traffico HTTPS con il comando CLI **config network web-auth https-redirect enable.**
>
> Questo usa molte risorse per il WLC nei casi in cui vengono inviate molte richieste HTTPS. Non è consigliabile utilizzare questa funzionalità prima della versione WLC 8.7, in cui la scalabilità di questa funzionalità è stata migliorata. Si noti inoltre che in questo caso è inevitabile un avviso di certificato. Se il client richiede un URL (ad esempio https://www.cisco.com), il WLC presenta comunque il proprio certificato rilasciato per l'indirizzo IP dell'interfaccia virtuale. Questo indirizzo non corrisponde mai all'URL/IP richiesto dal client e il certificato non è attendibile a meno che il client non imponga l'eccezione nel browser.

Calo indicativo delle prestazioni della versione del software WLC precedente alla 8.7 misurato:

Webauth	Velocità raggiunta
3 URL - HTTP	140/s
1° URL - HTTP Secondo e terzo URL - HTTPS	20/s
3 URL - HTTPS (distribuzione di grandi dimensioni)	<1/secondo
3 URL - HTTPS (massimo 100 client)	10/s

In questa tabella delle prestazioni, i 3 URL sono indicati come:

- URL originale immesso dall'utente finale
- URL a cui il WLC reindirizza il browser
- Invio finale delle credenziali

La tabella delle prestazioni fornisce le prestazioni del WLC se tutti e 3 gli URL sono HTTP, se tutti e 3 gli URL sono HTTPS o se il client si sposta da HTTP a HTTPS (tipico).

Come utilizzare una pagina interna (locale) con WebAuth

Per configurare una WLAN con un'interfaccia dinamica operativa, i client ricevono anche un indirizzo IP del server DNS tramite DHCP.

Prima di qualsiasi **webauth** , è impostata, verificare che la WLAN funzioni correttamente, che le richieste DNS possano essere risolte (**nslookup**) e le pagine Web possono essere visualizzate.

Impostare l'autenticazione Web come funzionalità di protezione di livello 3. Creare utenti nel database locale o in un server RADIUS esterno.

Fare riferimento al documento di esempio relativo alla configurazione dell'autenticazione Web di Wireless LAN Controller.

Come configurare un oggetto WebAuth locale personalizzato con una pagina personalizzata

Personalizzato **webauth** può essere configurato con **redirectUrl** dal **Security** . Verrà forzato il reindirizzamento a una pagina Web specifica immessa.

Quando l'utente viene autenticato, sostituisce l'URL originale richiesto dal client e visualizza la pagina per cui è stato assegnato il reindirizzamento.

La funzionalità personalizzata consente di utilizzare una pagina HTML personalizzata anziché la pagina di accesso predefinita. Caricare il pacchetto di file HTML e immagine sul controller.

Nella pagina di caricamento, cerca **webauth bundle** in formato tar. PicoZip crea tars compatibili con il WLC.

Per un esempio di bundle WebAuth, consultare la pagina Download Software for Wireless Controller WebAuth Bundle. Selezionare la versione appropriata per il WLC.

Si consiglia di personalizzare un fascio esistente; non create un nuovo fascio.

Esistono alcune limitazioni per **custom webauth** che variano a seconda delle versioni e dei bug.

- le dimensioni del file .tar (non più di 5 MB)
- numero di file nel file .tar
- la lunghezza del nome dei file (non più di 30 caratteri)

Se il pacchetto non funziona, provare a creare un pacchetto personalizzato semplice. Aggiungere singolarmente file e complessità per raggiungere il pacchetto che l'utente ha tentato di utilizzare. Questo aiuta a identificare il problema.

Per configurare una pagina personalizzata, vedere Creazione di una pagina di accesso con autenticazione Web personalizzata, sezione della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.6.

Sostituisci tecnica di configurazione globale

Eseguire la configurazione con il comando **override global config** e impostare un tipo WebAuth per ciascuna WLAN. In questo modo viene autorizzato un WebAuth interno/predefinito con un WebAuth interno/predefinito personalizzato per un'altra WLAN.

Ciò consente di configurare pagine personalizzate diverse per ciascuna WLAN.

Combina tutte le pagine nello stesso bundle e caricale sul WLC.

Impostare la pagina personalizzata con il comando **override global config** su ciascuna WLAN e selezionare il file che rappresenta la pagina di login da tutti i file all'interno del bundle.

Scegliere una pagina di accesso diversa all'interno del bundle per ciascuna WLAN.

Problema di reindirizzamento

All'interno del bundle HTML è presente una variabile che consente il reindirizzamento. Non inserire qui l'URL di reindirizzamento forzato.

Per i problemi di reindirizzamento in WebAuth personalizzato, Cisco consiglia di controllare il bundle.

Se si immette un URL di reindirizzamento con **+=** nell'interfaccia utente del WLC, l'URL potrebbe essere sovrascritto *o* aggiunto all'URL definito all'interno del bundle.

Ad esempio, nell'interfaccia utente del WLC, **redirectURL** è impostato su www.cisco.com; tuttavia, nel fascio indica: **redirectURL+=** '(URL sito Web)'. Il segno **+=** reindirizza gli utenti a un URL non valido.

Come utilizzare l'autenticazione Web esterna (locale) con una pagina esterna

L'utilizzo di un server WebAuth esterno è solo un repository esterno per la pagina di accesso. Le credenziali utente sono ancora autenticate dal WLC. Il server Web esterno consente solo una pagina di accesso speciale o diversa.

Passi eseguiti per un WebAuth esterno:

1. Il client (utente finale) apre un browser Web e immette un URL.

2. Se il client non è autenticato e viene utilizzata l'autenticazione Web esterna, il WLC reindirizza l'utente all'URL del server Web esterno. Il WLC invia un reindirizzamento HTTP al client con l'indirizzo IP imitato e punta all'indirizzo IP del server esterno. All'URL di accesso per l'autenticazione Web esterna vengono aggiunti parametri quali **AP_Mac_Address**,OSPF (Open Shortest Path First) **client_url** (**indirizzo URL client**) e **action_URL** per contattare il server web dello switch.

3. L'URL del server Web esterno invia l'utente a una pagina di accesso. L'utente può utilizzare un elenco di controllo di accesso (ACL) di preautenticazione per accedere al server.

4. La pagina di accesso invia la richiesta di credenziali utente al **action_URL**come http://192.0.2.1/login.html, del server Web WLC. Viene fornito come parametro di input per l'URL di reindirizzamento, dove 192.0.2.1 è l'indirizzo dell'interfaccia virtuale sullo switch.

5. Il server Web WLC invia il nome utente e la password per l'autenticazione.

6. Il WLC avvia la richiesta del server RADIUS o utilizza il database locale sul WLC, quindi autentica l'utente.

7. Se l'autenticazione ha esito positivo, il server Web WLC inoltra l'utente all'URL di reindirizzamento configurato o all'URL immesso dal client.

8. Se l'autenticazione non riesce, il server Web WLC reindirizza l'utente all'URL di accesso dell'utente.

   Nota: in questo documento, si usa 192.0.2.1 come esempio di ip virtuale. Si consiglia di usare l'intervallo 192.0.2.x per l'ip virtuale perché non è instradabile. La documentazione precedente fa riferimento alla versione "1.1.1.x" o è ancora quella configurata nel WLC come impostazione predefinita. Tuttavia, notare che ora questo indirizzo IP è un indirizzo IP instradabile valido e quindi si consiglia la subnet 192.0.2.x.

Se gli access point sono in modalità FlexConnect, viene **preauth** L'ACL è irrilevante. È possibile utilizzare gli ACL Flex per consentire l'accesso al server Web ai client non autenticati.

Fare riferimento all'esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless.

Pass-through Web

Web PassThrough è una variante dell'autenticazione Web interna. Visualizza una pagina con un avviso o un'istruzione di avviso, ma non richiede credenziali.

L'utente quindi fa clic su **ok**. Abilitare l'input e-mail e l'utente può immettere il proprio indirizzo e-mail che diventa il proprio nome utente.

Quando l'utente è connesso, controllare l'elenco dei client attivi e verificare che l'utente sia elencato con l'indirizzo di posta elettronica immesso come nome utente.

Per ulteriori informazioni, fare riferimento all'esempio di configurazione del passthrough Web del controller LAN wireless 5760/3850.

Reindirizzamento Web condizionale

Se si abilita un reindirizzamento Web condizionale, l'utente verrà reindirizzato in modo condizionale a una pagina Web specifica dopo il completamento dell'autenticazione 802.1x.

Èpossibile specificare la pagina di reindirizzamento e le condizioni in cui si verifica il reindirizzamento sul server RADIUS.

Le condizioni possono includere la password quando raggiunge la data di scadenza o quando l'utente deve pagare una fattura per continuare a utilizzare/accedere.

Se il server RADIUS restituisce la coppia AV Cisco **url-redirect**, quindi l'utente viene reindirizzato all'URL specificato quando apre un browser.

Se il server restituisce anche la coppia Cisco AV **url-redirect-acl**, l'ACL specificato viene installato come ACL di preautenticazione per questo client.

A questo punto, il client non è considerato completamente autorizzato e può solo passare il traffico consentito dall'ACL di preautenticazione. Dopo che il client ha completato una determinata operazione all'URL specificato (ad esempio, una modifica della password o il pagamento di una fattura), deve eseguire nuovamente l'autenticazione.

Quando il server RADIUS non restituisce un **url-redirect**, il client viene considerato completamente autorizzato e autorizzato a superare il traffico.

> **Nota:** La funzione di reindirizzamento Web condizionale è disponibile solo per le WLAN configurate per la sicurezza di layer 2 802.1x o WPA+WPA2.

Dopo la configurazione del server RADIUS, configurare il reindirizzamento Web condizionale sul controller con l'interfaccia utente grafica o la CLI del controller. Fare riferimento alle seguenti guide dettagliate: Configurazione di Web Redirect (GUI) e Configurazione di Web Redirect (CLI).

Reindirizzamento Web pagina iniziale

Se si abilita il reindirizzamento Web della pagina iniziale, l'utente verrà reindirizzato a una pagina Web specifica dopo il completamento dell'autenticazione 802.1x. Dopo il reindirizzamento, l'utente ha accesso completo alla rete.

Èpossibile specificare la pagina di reindirizzamento sul server RADIUS. Se il server RADIUS restituisce la coppia AV Cisco **url-redirect**, quindi l'utente viene reindirizzato all'URL specificato quando apre un browser.

A questo punto, il client è considerato completamente autorizzato e può passare il traffico, anche se il server RADIUS non restituisce un **url-redirect**.

> **Nota:** La funzione di reindirizzamento della pagina iniziale è disponibile solo per le WLAN configurate per la sicurezza di layer 2 802.1x o WPA+WPA2.

Dopo aver configurato il server RADIUS, configurare il reindirizzamento Web della pagina iniziale sul controller con la GUI o la CLI del controller.

Errore di WebAuth su filtro MAC

WebAuth su errore filtro MAC richiede di configurare i filtri MAC nel menu di protezione di layer 2.

Se gli utenti vengono convalidati con i propri indirizzi MAC, accedono direttamente al **run** state.

Se non lo sono, allora vanno al **WEBAUTH_REQD** e viene eseguita la normale autenticazione web.

> **Nota:** Questa condizione non è supportata con la funzionalità Web pass-through.Per ulteriori informazioni, seguire l'attività sulla richiesta di miglioramento, ID bug Cisco CSCtw73512

Autenticazione Web centrale

L'autenticazione Web centrale si riferisce a uno scenario in cui il WLC non ospita più alcun servizio. Il client viene inviato direttamente al portale Web di ISE e non attraversa la versione 192.0.2.1 sul WLC. La pagina di accesso e l'intero portale vengono esternalizzati.

L'autenticazione Web centrale ha luogo quando si abilita RADIUS Network Admission Control (NAC) nelle impostazioni avanzate dei filtri WLAN e MAC.

Il WLC invia un'autenticazione RADIUS (generalmente per il filtro MAC) ad ISE, che risponde con il **redirect-url** coppia di valori attributo (AV).

L'utente viene quindi inserito **POSTURE_REQD** finché ISE non fornisce l'autorizzazione con una richiesta di modifica dell'autorizzazione (CoA). Lo stesso scenario si verifica in Posture o Central WebAuth.

Central WebAuth non è compatibile con WPA-Enterprise/802.1x perché il portale guest non può restituire chiavi di sessione per la crittografia come nel caso di EAP (Extensible Authentication Protocol).

Autenticazione utente esterno (RADIUS)

L'autenticazione utente esterno (RADIUS) è valida solo per Local WebAuth quando WLC gestisce le credenziali o quando è abilitato un criterio Web di layer 3. Autenticazione degli utenti in locale o sul WLC o esternamente tramite RADIUS.

Il WLC controlla le credenziali dell'utente in un ordine specifico.

1. In ogni caso, prima cerca nel proprio database.
2. Se non trova gli utenti, va al server RADIUS configurato nella WLAN guest (se ne è stato configurato uno).
3. Viene quindi eseguito il Check-In dell'elenco globale dei server RADIUS in base ai server RADIUS in cui **network user** è selezionato.

Questo terzo punto risponde alla domanda di coloro che non configurano RADIUS per quella WLAN, ma notano che controlla ancora il RADIUS quando l'utente non viene trovato sul controller.

Questo perché **network user** viene confrontato con i server RADIUS nell'elenco globale.

WLC può autenticare gli utenti al server RADIUS con Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) o EAP-MD5 (Message Digest5).

Questo è un parametro globale ed è configurabile dalla GUI o dalla CLI:

Dalla GUI: passare a **Controller > Web RADIUS Authentication**

Dalla CLI: inserire **config custom-web RADIUSauth**

> Nota:il server guest NAC utilizza solo PAP.

Come impostare una WLAN guest cablata

Una configurazione WLAN guest cablata è simile a una configurazione guest wireless. Può essere configurato con uno o due controller (solo se uno è ad ancoraggio automatico).

Scegliere una VLAN come VLAN per gli utenti guest con cavo, ad esempio, sulla VLAN 50. Quando un utente guest con cavo desidera accedere a Internet, collegare il notebook a una porta su uno switch configurato per la VLAN 50.

Questa VLAN 50 deve essere consentita e presente sul percorso tramite la porta trunk WLC.

In un caso di due WLC (un'ancora e una esterna), questa VLAN guest cablata deve condurre al WLC esterno (denominato WLC1) e non all'ancora.

WLC1 si occupa quindi del tunnel del traffico verso il WLC della DMZ (l'ancora, chiamata WLC2), che rilascia il traffico nella rete indirizzata.

Di seguito sono riportati i cinque passaggi per configurare l'accesso guest cablato:

1. Configurare un'interfaccia dinamica (VLAN) per l'accesso degli utenti guest con cavo.

   Su WLC1, creare un'interfaccia dinamica VLAN50. Nel **interface configuration** , controllare la **Guest LAN** casella. Quindi, campi quali **IP address** e **gateway** scomparire. Il WLC deve riconoscere che il traffico è instradato dalla VLAN 50. Questi client sono guest cablati.

2. Creare una LAN cablata per l'accesso degli utenti guest.

   Su un controller, viene usata un'interfaccia quando associata a una WLAN. Quindi, creare una WLAN sui controller dell'ufficio principale. Passa a **WLANs** e fare clic su **New**. Dentro **WLAN Type**, scegliere **Guest LAN**.

   In Nome profilo e SSID WLAN, immettere un nome che identifichi la WLAN. I nomi possono essere diversi, ma non possono contenere spazi. Viene utilizzato il termine WLAN, ma questo profilo di rete non è correlato al profilo di rete wireless.

   OSPF (Open Shortest Path First) **General** In questa scheda sono disponibili due elenchi a discesa: **Ingress** e **Egress**. In entrata è la VLAN da cui provengono gli utenti (VLAN 50); In uscita è la VLAN a cui vengono inviati.

   Per **Ingress**, scegliere **VLAN50**.

   Per **Egress**, è diverso. Se si dispone di un solo controller, creare un'altra interfaccia dinamica, **standard** una volta (non una LAN guest) e inviare gli utenti cablati a questa interfaccia. In questo caso, inviarli al controller DMZ. Pertanto, per **Egress** , scegliere il **Management Interface**.

   OSPF (Open Shortest Path First) **Security** La modalità per questa rete WLAN guest è WebAuth, il che è accettabile. Clic **Ok** per la convalida.

3. Configurare il controller esterno (ufficio principale).

Dal **WLAN list**, fare clic su **Mobility Anchor** alla fine del **Guest LAN** e scegliere il controller DMZ. Si presume che entrambi i controller si riconoscano a vicenda. In caso contrario, visitare il sito **Controller** > **Mobility Management** > **Mobility group**, e aggiungere **DMZWLC** su WLC1. Quindi aggiungere **WLC1** su DMZ. Entrambi i controller non devono appartenere allo stesso gruppo di mobilità. In caso contrario, vengono violate le regole di sicurezza di base.

4. **Configurare il controller di ancoraggio (il controller DMZ).**

   Il controller dell'ufficio principale è pronto. Preparare il controller DMZ. Aprire una sessione del browser Web sul controller DMZ e selezionare **WLAN**. Creare una nuova WLAN. Dentro **WLAN Type**, scegliere **Guest LAN**.

   Dentro **Profile Name** e **WLAN SSID**, immettere un nome che identifichi la WLAN. Utilizzare gli stessi valori immessi nel controller dell'ufficio principale.

   OSPF (Open Shortest Path First) **Ingress** interfaccia **None**. Non importa perché il traffico viene ricevuto tramite il tunnel Ethernet over IP (EoIP). Non è necessario specificare un'interfaccia in ingresso.

   OSPF (Open Shortest Path First) **Egress** dove devono essere inviati i client. Ad esempio, la **DMZ VLAN** è la VLAN 9. Creare un'interfaccia dinamica standard per la VLAN 9 sul DMZWLC, quindi scegliere **VLAN 9** come interfaccia di uscita.

   Configurare l'estremità del tunnel Mobility Anchor. Dall'**elenco WLAN**, scegliere **Mobility Anchor for Guest LAN**. Inviare il traffico al controller locale **DMZWLC**. Entrambe le estremità sono pronte.

5. **Ottimizzare la LAN guest.**

   Inoltre, è possibile regolare le impostazioni WLAN su entrambe le estremità. Le impostazioni devono essere identiche su entrambe le estremità. Ad esempio, se si fa clic sul pulsante **WLAN Advanced** , **Allow AAA override** su WLC1, selezionare la stessa casella su DMZWLC. In caso di differenze nella WLAN su entrambi i lati, il tunnel si interrompe. DMZWLC rifiuta il traffico; è possibile vedere quando **run debug mobility**.

   Tenete presente che tutti i valori sono effettivamente ottenuti da DMZWLC: indirizzi IP, valori VLAN e così via. Configurare il lato WLC1 in modo identico, in modo che inoltri la richiesta al WLCDMZ.

Certificati per la pagina di accesso

In questa sezione vengono illustrati i processi per inserire il proprio certificato nella pagina WebAuth o per nascondere l'URL WebAuth 192.0.2.1 e visualizzare un URL denominato.

Carica un certificato per l'autenticazione Web del controller

Tramite GUI (**WebAuth > Certificate**) o CLI (tipo di trasferimento **webauthcert**) è possibile caricare un certificato sul controller.

Sia che si tratti di un certificato creato con l'Autorità di certificazione (CA) dell'utente o di un certificato ufficiale di terze parti, deve essere in formato .pem.

Prima di inviare, è necessario immettere anche la chiave del certificato.

Dopo il caricamento, è necessario riavviare il sistema per rendere effettivo il certificato. Una volta riavviato, andare alla pagina WebAuth del certificato nella GUI per trovare i dettagli del certificato caricato (validità e così via).

Il campo importante è il nome comune (CN), che è il nome assegnato al certificato. Questo campo viene trattato in questo documento nella sezione "Certificati di autorità e altri certificati sul controller".

Dopo il riavvio e la verifica dei dettagli del certificato, viene visualizzato il nuovo certificato del controller nella pagina di accesso di WebAuth. Tuttavia, possono verificarsi due situazioni.

1. Se il certificato è stato rilasciato da una delle poche CA principali considerate attendibili da tutti i computer, non vi sono problemi. Un esempio è VeriSign, ma in genere si è firmati da una CA secondaria di Verisign e non dalla CA radice. È possibile archiviare l'archivio certificati del browser se la CA indicata è attendibile.

2. Se il certificato proviene da una società o una CA più piccola, tutti i computer non sono considerati attendibili. Fornire il certificato della società o della CA anche al client e una delle CA radice rilascia tale certificato. Alla fine, si dispone di una catena come "Il certificato è stato rilasciato da CA x > CA x il certificato è stato emesso da CA y > CA y il certificato è stato emesso da questa CA radice attendibile". L'obiettivo finale è quello di raggiungere una CA considerata attendibile dal client.

Certificati di autorità e altri certificati sul controller

Per eliminare l'avviso "questo certificato non è attendibile", immettere il certificato della CA che ha emesso il certificato del controller sul controller.

Il controller presenta quindi entrambi i certificati (il certificato del controller e il relativo certificato CA). Il certificato CA deve essere una CA attendibile o disporre delle risorse per verificare la CA. È possibile creare una catena di certificati CA che porti a una CA attendibile.

Posizionate l'intera catena nello stesso file. Il file include quindi contenuto simile al seguente:

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

Come fare in modo che il certificato corrisponda all'URL

L'URL WebAuth è impostato su 192.0.2.1 per autenticarsi e viene emesso il certificato (questo è il campo CN del certificato WLC).

Per modificare l'URL di WebAuth in 'myWLC.com', ad esempio, passare alla **virtual interface configuration** (l'interfaccia 192.0.2.1) e qui è possibile immettere un **virtual DNS hostname**, ad esempio myWLC.com.

Sostituisce la versione 192.0.2.1 della barra dell'URL. Anche questo nome deve essere risolvibile. La traccia dello sniffer mostra come funziona tutto, ma quando il WLC invia la pagina di accesso, il WLC mostra l'indirizzo myWLC.com e il client risolve questo nome con il proprio DNS.

Il nome deve avere la risoluzione 192.0.2.1. Ciò significa che se si usa anche un nome per la gestione del WLC, usare un nome diverso per WebAuth.

Se si utilizza myWLC.com mappato all'indirizzo IP di gestione WLC, è necessario utilizzare un nome diverso per WebAuth, ad esempio myWLCwebauth.com.

Risoluzione dei problemi relativi ai certificati

In questa sezione vengono illustrati i metodi e gli elementi da controllare per risolvere i problemi relativi ai certificati.

Modalità di verifica

Scaricare OpenSSL (per Windows, cercare OpenSSL Win32) e installarlo. Senza alcuna configurazione, è possibile accedere alla directory bin e provare **openssl s_client –connect (your web auth URL):443**,

se questo URL è l'URL al quale la pagina WebAuth è collegata sul DNS, vedere "What to Check" nella sezione successiva di questo documento.

Se i certificati utilizzano una CA privata, posizionare il certificato CA radice in una directory di un computer locale e utilizzare l'opzione openssl **-CApath**. Se si dispone di una CA intermedia, inserirla anche nella stessa directory.

Per ottenere informazioni generali sul certificato e per verificarlo, utilizzare:

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

Èinoltre utile convertire i certificati utilizzando openssl:

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

Cosa controllare

Èpossibile visualizzare i certificati inviati al client al momento della connessione. Leggere il certificato del dispositivo — il CN deve essere l'URL in cui è raggiungibile la pagina Web.

Leggere la riga "rilasciato da" del certificato del dispositivo. Deve corrispondere al CN del secondo certificato. Questo secondo certificato, "rilasciato da", deve corrispondere al CN del certificato successivo e così via. Altrimenti, non crea una catena reale.

Nell'output OpenSSL mostrato di seguito, notare che **openssl** impossibile verificare il certificato del dispositivo perché il relativo "rilasciato da" non corrisponde al nome del certificato CA fornito.

Output SSL

```
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)
---
```

Èinoltre possibile che il certificato non possa essere caricato nel controller. In questa situazione non c'è questione di validità, CA, e così via.

Per verificare questa condizione, controllare la connettività TFTP (Trivial File Transfer Protocol) e provare a trasferire un file di configurazione. Se si immette il **debug transfer all enable** notare che il problema è l'installazione del certificato.

Ciò potrebbe essere dovuto alla chiave errata utilizzata con il certificato. È inoltre possibile che il certificato sia in un formato errato o sia danneggiato.

Cisco consiglia di confrontare il contenuto del certificato con un certificato noto e valido. Ciò consente di verificare se un **LocalkeyID** l'attributo mostra tutti gli 0 (già eseguito). In tal caso, il certificato deve essere riconvertito.

Con OpenSSL sono disponibili due comandi che consentono di tornare da .pem a .p12, quindi di riemettere un .pem con la chiave desiderata.

Se si riceve un file con estensione pem contenente un certificato seguito da una chiave, copiare/incollare la parte della chiave: **----BEGIN KEY ---- until ------- END KEY ------** dal file .pem in "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? Viene visualizzata una chiave; inserire **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** Il risultato è un file .pem operativo con la password **check123**.

Altre situazioni da risolvere

Sebbene **mobility anchor** non sia stato discusso in questo documento, se si è in una situazione **guest ancorata**, assicurarsi che lo scambio di mobilità avvenga correttamente e che si veda il client arrivare sull'ancoraggio.

Per qualsiasi altro problema relativo a WebAuth è necessario risolvere il problema dell'ancoraggio.

Di seguito sono riportati alcuni problemi comuni che è possibile risolvere:

- **Gli utenti non possono associarsi alla WLAN guest**.

  Non è correlato a WebAuth. Controllare la configurazione del client, le impostazioni di sicurezza sulla WLAN, se è abilitata, se le radio sono attive e operative e così via.

- **Gli utenti non ottengono l'indirizzo IP**.

  In una situazione di ancoraggio ospite, questo è il più delle volte perché l'ancoraggio straniero non era configurato esattamente allo stesso modo. In caso contrario, controllare la configurazione DHCP, la connettività e così via.
- Confermare se altre WLAN possono usare lo stesso server DHCP senza problemi. Non è ancora correlato a WebAuth.

- **L'utente non viene reindirizzato alla pagina di accesso**.

  Questo è il sintomo più comune, ma è più preciso. Ci sono due possibili scenari.

  L'utente non viene reindirizzato (l'utente immette un URL e non raggiunge mai la pagina WebAuth). In questo caso, controllare:

  che un server DNS valido è stato assegnato al client tramite DHCP (**ipconfig /all**),

  che il DNS sia raggiungibile dal client (**nslookup (website URL**),

  l'utente ha immesso un URL valido per il reindirizzamento,

  il fatto che l'utente si sia connesso a un URL HTTP sulla porta 80 (ad esempio, per raggiungere un ACS con http://localhost:2002 non comporta il reindirizzamento poiché l'utente

ha inviato un messaggio sulla porta 2002 anziché 80).

L'utente viene reindirizzato correttamente a 192.0.2.1, ma la pagina stessa non viene visualizzata.

Questa situazione può essere dovuta a un problema del WLC o a un problema del client. È possibile che il client disponga di un firewall, di un software o di un blocco di criteri. È inoltre possibile che abbiano configurato un proxy nel browser Web.

Raccomandazione: Traccia di uno sniffer sul PC client. Non è necessario un software wireless speciale, solo Wireshark, che viene eseguito sulla scheda di rete wireless e mostra se il WLC risponde e cerca di reindirizzare. Sono disponibili due possibilità: non è stata ricevuta alcuna risposta dal WLC o si è verificato un errore nell'handshake SSL per la pagina WebAuth. Per il problema dell'handshake SSL, è possibile controllare se il browser utente consente SSLv3 (alcune consentono solo SSLv2) e se è troppo aggressivo durante la verifica del certificato.

Ènormale immettere manualmente http://192.0.2.1 per verificare se la pagina Web viene visualizzata senza DNS. In realtà, è possibile digitare http://10.0.0.0 e ottenere lo stesso effetto. Il WLC reindirizza qualsiasi indirizzo IP immesso. Pertanto, se si immette http://192.0.2.1, non è possibile aggirare il reindirizzamento Web. Se si immette https://192.0.2.1(sicuro), l'operazione non funzionerà perché il WLC non reindirizza il traffico HTTPS (per impostazione predefinita, questa condizione è possibile in realtà nella versione 8.0 e successive). Il modo migliore per caricare la pagina direttamente senza un reindirizzamento è immettere https://192.0.2.1/login.html.

- **Gli utenti non possono eseguire l'autenticazione**.

  Vedere la sezione di questo documento in cui viene descritta l'autenticazione. Controllare le credenziali localmente sul RADIUS.

- **Gli utenti possono eseguire l'autenticazione tramite WebAuth, ma successivamente non dispongono dell'accesso a Internet**.

  Èpossibile rimuovere WebAuth dalla sicurezza della WLAN e quindi avere una WLAN aperta. È quindi possibile provare ad accedere al Web, al DNS e così via. In caso di problemi, rimuovere completamente le impostazioni WebAuth e controllare la configurazione delle interfacce.

Per ulteriori informazioni, fare riferimento a: Risoluzione dei problemi di autenticazione Web su un controller WLC.

Server proxy HTTP e relativo funzionamento

Èpossibile utilizzare un server proxy HTTP. Se è necessario che il client aggiunga un'eccezione nel browser che 192.0.2.1 non deve passare attraverso il server proxy, è possibile fare in modo che il WLC ascolti il traffico HTTP sulla porta del server proxy (generalmente 8080).

Per comprendere questo scenario, è necessario conoscere la funzione di un proxy HTTP. Si tratta

di un'opzione configurata sul lato client (indirizzo IP e porta) nel browser.

Lo scenario tipico in cui un utente visita un sito Web è quello di risolvere il nome in IP con DNS e quindi di chiedere alla pagina Web di accedere al server Web. Il processo invia sempre la richiesta HTTP per la pagina al proxy.

Il proxy elabora il DNS, se necessario, e lo inoltra al server Web (se la pagina non è già memorizzata nella cache del proxy). La discussione è solo da client a proxy. Il fatto che il proxy ottenga o meno la pagina web reale è irrilevante per il cliente.

Processo di autenticazione Web:

- L'utente digita un URL.
- Il PC client invia al server proxy.
- WLC intercetta e imita l'IP del server proxy; risponde al PC con un reindirizzamento a 192.0.2.1

In questa fase, se il PC non è configurato per questo, viene richiesta la pagina 192.0.2.1 WebAuth al proxy in modo che non funzioni. Il PC deve fare un'eccezione per 192.0.2.1; quindi invia una richiesta HTTP a 192.0.2.1 e procede con WebAuth.

Una volta autenticate, tutte le comunicazioni passano di nuovo attraverso il proxy. Una configurazione di eccezione si trova in genere nel browser vicino alla configurazione del server proxy. Viene quindi visualizzato il messaggio: "Non utilizzare il proxy per questi indirizzi IP".

Con WLC release 7.0 e successive, la funzione **webauth proxy redirect** possono essere abilitati nelle opzioni di configurazione WLC globali.

Quando è abilitato, il WLC controlla se i client sono configurati per utilizzare manualmente un proxy. In tal caso, reindirizzano il client a una pagina che mostra loro come modificare le loro impostazioni proxy per far funzionare tutto.

Il reindirizzamento del proxy WebAuth può essere configurato per funzionare su un'ampia gamma di porte ed è compatibile con l'autenticazione Web centrale.

Per un esempio sul reindirizzamento del proxy WebAuth, fare riferimento all'esempio di configurazione del proxy di autenticazione Web su un controller LAN wireless.

Autenticazione Web su HTTP anziché su HTTPS

Èpossibile accedere all'autenticazione Web su HTTP anziché su HTTPS. Se si accede a HTTP, non si riceveranno avvisi sui certificati.

Per il codice precedente alla release 7.2 di WLC, è necessario disabilitare la gestione HTTPS del WLC e uscire dalla gestione HTTP. Tuttavia, questa opzione consente solo la gestione Web del WLC su HTTP.

Per il codice WLC release 7.2, utilizzare il **config network web-auth secureweb disable** da disattivare. In questo modo viene disabilitato solo HTTPS per l'autenticazione Web e non per la gestione. È necessario riavviare il controller.

Sul codice WLC release 7.3 e successive, è possibile abilitare/disabilitare HTTPS per WebAuth solo tramite GUI e CLI.

Informazioni correlate

- Esempio di configurazione dell'autenticazione Web del controller LAN wireless
- Scarica il software per i bundle WebAuth dei controller wireless
- Creazione di una pagina di accesso con autenticazione Web personalizzata
- Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless
- Esempio di configurazione del controller LAN wireless 5760/3850 Web Passthrough
- Configurazione di Web Redirect (GUI)
- Configurazione di Web Redirect (CLI)
- Risoluzione dei problemi di autenticazione Web su un controller WLC
- Esempio di configurazione del proxy di autenticazione Web su un controller LAN wireless
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).