Authentification Web sur le contrôleur WLAN

Contenu

Introduction

Ce document explique les procédés pour l'authentification Web sur un contrôleur LAN Sans fil (WLC).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de base de la configuration WLC.

Composants utilisés

Les informations dans ce document sont basées sur tous les modèles matériels WLC.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Procédés intérieurs d'authentification Web

Position d'authentification Web comme fonctionnalité de sécurité

L'authentification Web (WebAuth) est degré de sécurité de la couche 3. Il tient compte de la Sécurité conviviale qui travaille à n'importe quelle station qui exécute un navigateur. Il peut également être combiné avec n'importe quelle Sécurité (PSK) principale pré-partagée (stratégie de sécurité de couche 2). Bien que la combinaison de WebAuth et de PSK réduise la partie conviviale de manière significative et ne soit pas utilisée souvent, elle a toujours l'avantage pour chiffrer le trafic de client. WebAuth est une méthode d'authentification sans cryptage.

WebAuth ne peut pas être configuré avec 802.1x/RADIUS (Remote Authentication Dial-In User Service) jusqu'à ce que la version de logiciel 7.4 WLC soit installée où elle peut être configurée en même temps. Cependant, rendez-vous compte que les clients doivent passer par le dot1x et l'authentification Web. On ne le signifie pas pour l'invité, mais pour l'ajout d'un portail web pour des employés (qui 802.1x d'utilisation). Il n'y a pas un Identifiant SSID (Service Set Identifier) tout-en-un pour le dot1x pour des employés ou le portail web pour des invités.

Comment WebAuth fonctionne

La procédure d'authentification de 802.11 est ouverte, ainsi vous pouvez authentifier et s'associer sans problème. Après cela, vous êtes associé, mais pas dans l'état de **PASSAGE** WLC. L'authentification Web étant activé, vous êtes maintenu dans **WEBAUTH_REQD** où vous ne pouvez accéder à aucune ressource de réseau (aucun ping, et ainsi de suite). Vous devez recevoir une adresse IP DHCP avec l'adresse du serveur DNS dans les options.

Vous devez taper un URL valide en votre navigateur. Le client résout l'URL par le protocole DNS. Le client envoie alors sa demande de HTTP à l'adresse IP du site Web. Les interceptions WLC qui demandent et renvoient la page de connexion de **webauth**, qui charrie l'adresse IP de site Web. Dans le cas d'un WebAuth externe, le WLC répond avec une réponse de HTTP qui inclut votre adresse IP de site Web et déclare que la page s'est déplacée. La page a été déplacée au web server externe utilisé par le WLC. Quand vous êtes authentifié, vous accédez à toutes les ressources de réseau et êtes réorienté à l'URL initialement prié, par défaut (à moins qu'un obligatoire réoriente était configuré sur le WLC). En résumé, le WLC permet au client pour résoudre les DN et pour obtenir une adresse IP automatiquement dans l'état **WEBAUTH_REQD**.

Conseil : Si vous voulez que le WLC observe un autre port au lieu du port 80, vous pouvez employer le **number> de <port de config network web-auth-port** pour créer une réorientation sur ce port également. Un exemple est l'interface web du serveur de contrôle d'accès (ACS), qui est sur des applications semblables de port 2002 ou autre.

Note au sujet de redirection HTTPS : Par défaut et dans les versions 7.x et plus tôt, le WLC n'a pas réorienté le trafic HTTPS. Ceci signifie que si vous ouvrez votre navigateur et tapez une adresse HTTPS, rien ne se produit. Vous devez taper une adresse HTTP afin d'obtenir réorienté à la page de connexion qui a été servie dans HTTPS.

Dans la version 8.0 et ultérieures, vous pouvez activer la redirection du trafic HTTPS avec le **Web-auth de réseau de config de** commande CLI https-**réorientez l'enable.**

Rendez-vous compte que c'est ressource consommant pour le WLC au cas où beaucoup de demandes HTTPS seraient envoyées. Notez également qu'un avertissement de certificat est inévitable dans ce cas. En effet, si votre client demande tout URL (tel que https://www.cisco.com), le WLC présente toujours son propre certificat délivré pour l'adresse IP d'interface virtuelle. Ceci n'appariera évidemment jamais l'adresse IP URL demandée par le client et le certificat pas sont de confiance à moins que le client force l'exception en son navigateur.

Chute de performances indicative mesurée :

Webauth	**Débit réalisé**
3 URLs - HTTP	140/en second lieu
1er URL - HTTP 2ème et 3ème URLs - HTTPS	20/en second lieu
3 URLs - HTTPS (grand déploiement)	<1/en second lieu
3 URLs - HTTPS (maximum de 100 clients)	10/en second lieu

Dans cette table de représentation, les 3 URLs sont mentionnés en tant que :

- L'URL d'original est entré par l'utilisateur (le site Web que l'utilisateur veut parcourir à)
- L'URL le WLC réoriente le navigateur à
- L'envoi final de qualifications

La table de représentation donne la représentation WLC au cas où chacun des 3 URLs serait HTTP, au cas où chacun des 3 URLs serait HTTPS, ou si le client se déplace du HTTP à HTTPS (le scénario plus typique).

Comment faire un travail (local) interne de WebAuth avec une page interne

Si vous devez configurer un WLAN avec une interface dynamique opérationnelle, les clients devraient également recevoir une adresse IP de serveur DNS par le DHCP. Avant que vous placiez n'importe quel **webauth**, vous devriez tester que votre WLAN fonctionne correctement, que vous pouvez résoudre des demandes de DN (**nslookup**), et que vous pouvez parcourir des pages Web. Puis, vous pouvez placer l'authentification Web comme fonctionnalités de sécurité de la couche 3. Vous pouvez créer vos utilisateurs dans la base de données locale ou sur un serveur RADIUS externe, par exemple. Référez-vous au document Sans fil d'exemple de configuration d'authentification Web de contrôleur LAN.

Comment configurer des gens du pays faits sur commande WebAuth avec la page faite sur commande

Le webauth fait sur commande peut être configuré avec le **redirectUrl de l'onglet Sécurité**. Ceci force un redirect to une page Web spécifique que vous écrivez. Quand l'utilisateur est authentifié, il ignore l'URL d'original le client demandé et affiche la page pour laquelle la réorientation a été assignée.

La caractéristique faite sur commande te permet pour utiliser une page HTML faite sur commande au lieu de la page de connexion par défaut. Téléchargez votre HTML et fichiers d'image empaquettent au contrôleur. Dans la page de téléchargement, recherchez le **paquet de webauth** dans un format de goudron. Habituellement, PicoZip crée les goudrons qui fonctionnent compatiblement avec le WLC. Pour un exemple d'un paquet de WebAuth, référez-vous à la page de logiciel de téléchargement pour des paquets de WebAuth de contrôleur sans-fil. Soyez sûr de sélectionner la release appropriée pour votre WLC. Une bonne recommandation est de personnaliser un paquet qui existe ; ne créez pas un à partir de zéro de paquet.

Il y a quelques limites avec le **webauth fait sur commande** qui varient avec des versions et des bogues. Les choses à surveiller incluent :

- la taille de fichier de .tar (pas plus que 5MB)
- le nombre de fichiers dans le .tar
- la longueur de nom du fichier des fichiers (devraient être pas plus de 30 caractères)

Si votre module de client ne fonctionne pas, essayer avec un module fait sur commande simple. Ajoutez alors les fichiers et la complexité un par un pour atteindre le module le client jugé pour utiliser. Ceci devrait vous aider à identifier le problème. Pour un exemple sur la façon dont configurer une page faite sur commande, référez-vous à créer une page de connexion personnalisée d'authentification Web, une section dans le guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0.

Technique de configuration globale de priorité

Pour chaque WLAN, vous configurez avec la commande de **configuration globale de priorité** et placez un type de WebAuth pour chaque WLAN. Ceci signifie que vous pouvez avoir un interne/par défaut WebAuth avec un interne/par défaut faits sur commande WebAuth pour un autre WLAN. Ceci te permet également pour configurer différentes pages faites sur commande pour chaque WLAN. Vous devez combiner toutes vos pages dans le même paquet et les télécharger au WLC. Puis, vous pouvez placer votre page faite sur commande avec la commande de **configuration globale de priorité** sur chaque WLAN et la sélectionner que le fichier est la page de connexion à partir de tous les fichiers dans le paquet. Vous pouvez choisir une page de connexion différente à l'intérieur du paquet pour chaque WLAN.

Question de redirection

Il y a une variable dans le paquet HTML qui permet la redirection. Ne mettez pas votre URL obligatoire de redirection là. Pour n'importe quelle redirection émet dans WebAuth fait sur commande, Cisco recommande de vérifier le paquet. Si vous écrivez un URL de réorientation avec **+=** dans le GUI WLC, ceci pourrait remplacer *ou* ajouter à l'URL défini à l'intérieur du paquet. Par exemple, dans le GUI WLC, le champ de **redirectURL** est placé à www.cisco.com ; cependant, dans le paquet il affiche : **redirectURL+=** « www.google.com ». **Le +=** réoriente des utilisateurs à www.cisco.comwww.google.com, qui est un URL non valide.

Comment faire un travail (local) externe d'authentification Web avec une page externe

Comme déjà brièvement expliqué, l'utilisation d'un serveur externe de WebAuth est juste un référentiel externe pour la page de connexion. Les identifiants utilisateurs sont encore authentifiés par le WLC. Le web server externe te permet seulement pour utiliser une page de connexion spéciale ou différente. Voici les étapes exécutées pour un WebAuth externe :

1. Le client (utilisateur final) ouvre un navigateur Web et écrit un URL.

2. Si le client n'est pas authentifié et authentification de Web externe est utilisé, le WLC réoriente l'utilisateur à l'URL externe de web server. En d'autres termes, le WLC envoie à un redirect to de HTTP le client avec l'adresse IP charriée du site Web et des points à l'adresse IP de serveur externe. L'URL d'authentication login de Web externe est ajouté avec des paramètres tels que l'**AP_Mac_Address**, le **client_url** (www.website.com), et l'**action_URL** ce les besoins des clients d'entrer en contact avec le web server de commutateur.

3. L'URL externe de web server envoie l'utilisateur à une page de connexion. Alors l'utilisateur peut employer une liste de contrôle d'accès de pré-authentification (ACL) afin d'accéder au serveur. L'ACL est nécessaire pour tous les modèles WLC excepté la gamme 4400 et le Wism1.

4. La page de connexion prend les identifiants utilisateurs entrés et envoie la demande de nouveau à l'**action_URL**, tel que http://1.1.1.1/login.html, du web server WLC. Ceci est fourni pendant qu'un paramètre d'entrée au client réorientent l'URL, où 1.1.1.1 est l'adresse d'interface virtuelle sur le commutateur.

5. Le web server WLC soumet le nom d'utilisateur et mot de passe pour l'authentification.

6. Le WLC initie la demande de serveur de RAYON ou utilise la base de données locale sur le WLC, et puis authentifie l'utilisateur.

7. Si l'authentification est réussie, le web server WLC l'un ou l'autre en avant l'utilisateur au configuré réorientent l'URL ou à l'URL le client est entré.

8. Si l'authentification échoue, alors le web server WLC réoriente l'utilisateur de nouveau à l'URL de procédure de connexion de client.

Remarque: Si les Points d'accès (aps) sont en mode de FlexConnect, un ACL de **preauth** est inutile. Le flexible ACLs peut être utilisé pour permettre l'accès au web server pour les clients qui n'ont pas été authentifiés. Référez-vous à l'authentification de Web externe avec l'exemple Sans fil de configuration de contrôleurs LAN.

Fonction émulation de Web

C'est une variation de l'authentification de Web interne. Il affiche une page avec une déclaration d'avertissement ou vigilante, mais n'incite pas pour des qualifications. L'utilisateur devrait cliquer sur l'**ok**. Vous pouvez permettre à l'email d'entrer, et l'utilisateur peut écrire leur adresse e-mail, qui

devient leur nom d'utilisateur. Quand l'utilisateur est connecté, vérifiez votre liste active de clients ; que l'utilisateur est répertorié avec l'adresse e-mail ils est entré comme nom d'utilisateur. Le pour en savoir plus, se rapportent à l'exemple Sans fil de configuration de fonction émulation de Web de contrôleur LAN.

Le Web conditionnel réorientent

Si vous activez un Web conditionnel réorientez, l'utilisateur est conditionnellement réorienté à une page Web particulière après que l'authentification de 802.1x se soit avec succès terminée. Vous pouvez spécifier la page de redirection et les conditions sous lesquelles celle-ci se produit sur votre serveur RADIUS. Les conditions peuvent inclure le mot de passe d'utilisateur quand il atteint la date d'expiration ou quand les besoins de l'utilisateur de payer une facture l'utilisation/accès continus. Si le serveur de RAYON renvoie la paire AV de Cisco URL-**réorientez**, alors l'utilisateur est réorienté à l'URL spécifié quand ils ouvrent un navigateur. Si le serveur renvoie également l'URL-réorienter-**acl de** paire AV de Cisco, alors l'ACL spécifié est installé comme ACL de pré-authentification pour ce client. Le client n'est pas considéré entièrement autorisé en ce moment et peut seulement passer le trafic permis par l'ACL de pré-authentification. Après que le client se termine une exécution particulière à l'URL spécifié (par exemple, une modification de mot de passe ou un paiement de facture), puis le client doit authentifier à nouveau. Quand le serveur de RAYON ne renvoie pas une URL-**réorientation**, le client est considéré entièrement autorisé et permis pour passer le trafic.

Remarque: Le Web conditionnel réorientent la caractéristique est disponible seulement pour les WLAN qui sont configurés pour le 802.1x ou WPA+WPA2 le degré de sécurité de la couche 2.

Après que vous configuriez le serveur de RAYON, vous pouvez alors configurer le Web conditionnel réorientez sur le contrôleur avec le GUI ou le CLI de contrôleur. Référez-vous à ces guides pas à pas : Utilisant le GUI pour configurer le Web réorientez et en employant le CLI pour configurer le Web réorientez.

Le Web de page de splash réorientent

Si vous activez le Web de page de splash réorientez, l'utilisateur est réorienté à une page Web particulière après que l'authentification de 802.1x se soit terminée avec succès. Après que la réorientation, l'utilisateur ait l'accès complet au réseau. Vous pouvez spécifier la page de réorientation sur votre serveur de RAYON. Si le serveur de RAYON renvoie la paire AV de Cisco URL-**réorientez**, alors l'utilisateur est réorienté à l'URL spécifié quand ils ouvrent un navigateur. Le client est considéré entièrement autorisé en ce moment et est permis pour passer le trafic, même si le serveur de RAYON ne renvoie pas une URL-**réorientation**.

Remarque: Le Web de page de splash réorientent la caractéristique est disponible seulement pour les WLAN qui sont configurés pour le 802.1x ou WPA+WPA2 le degré de sécurité de la couche 2.

Après que vous configuriez le serveur de RAYON, vous pouvez alors configurer le Web de page de splash réorientez sur le contrôleur avec le GUI ou le CLI de contrôleur.

WebAuth sur la panne de filtre d'adresses MAC

Ceci exige de vous de configurer des filtres d'adresses MAC sur le menu de degré de sécurité de la couche 2. Si des utilisateurs sont avec succès validés avec leurs adresses MAC, alors ils vont

directement à l'état de **passage**. S'ils ne sont pas, alors ils vont à l'état **WEBAUTH_REQD** et l'authentification Web normale se produit.

Remarque: Ceci n'est pas pris en charge avec la fonction émulation de Web. Le pour en savoir plus, suivent l'activité sur la demande d'amélioration CSCtw73512 .

Authentification Web centrale

L'authentification Web centrale se rapporte à un scénario où le WLC ne héberge plus aucun services. La différence réside dans le fait que le client est directement envoyé au portail web ISE et ne passe pas par 1.1.1.1 sur le WLC. La page de connexion et le portail entier sont extériorisés.

L'authentification Web centrale a lieu quand vous faites activer le Contrôle d'admission au réseau (NAC) de RAYON dans les paramètres avancés du WLAN et des filtres d'adresses MAC activés.

Le concept global est que le WLC envoie une authentification de RAYON (habituellement pour le filtre d'adresses MAC) à ISE, qui répond avec les paires de la valeur d'attribut réorienter-**URL** (poids du commerce). L'utilisateur est alors mis dans l'état **POSTURE_REQD** jusqu'à ce qu'ISE donne l'autorisation avec une modification de demande de l'autorisation (CoA). Le même scénario se produit à la posture ou au central WebAuth. WebAuth central n'est pas compatible avec WPA-Enterprise/802.1x parce que le portail d'invité ne peut pas renvoyer des clés de session pour le cryptage comme il fait avec le Protocole EAP (Extensible Authentication Protocol).

Authentification d'utilisateur externe (RAYON)

C'est seulement valide pour des gens du pays WebAuth quand WLC manipule les qualifications, ou quand une stratégie de Web de la couche 3 est activée. Vous pouvez alors authentifier des utilisateurs localement sur le WLC ou extérieurement par l'intermédiaire du RAYON.

Il y a une commande dans laquelle le WLC vérifie les qualifications de l'utilisateur.

1. En tous cas, il premier regarde dans sa propre base de données.
2. S'il ne trouve pas les utilisateurs là, il va au serveur de RAYON configuré dans le WLAN invité (s'il y a d'un configuré).
3. Il signe alors la liste globale de serveur de RAYON contre les serveurs de RAYON où l'**utilisateur du réseau** est vérifié.

Ce troisième point est très important et répond à la question de beaucoup qui ne configurent pas le RAYON pour ce WLAN, mais note qu'il vérifie toujours contre le RAYON quand l'utilisateur n'est pas trouvé sur le contrôleur. C'est parce que l'**utilisateur du réseau** est vérifié contre vos serveurs de RAYON dans la liste globale.

WLC peut authentifier des utilisateurs au serveur de RAYON avec le Password Authentication Protocol (PAP), le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) ou l'EAP-MD5 (message Digest5). C'est un paramètre global et est configurable du GUI ou du CLI :

Du GUI : naviguez **authentification** vers de **contrôleur** > de **Web RAYON**

Du CLI : écrivez le coutume-**Web RADIUSauth <pap|chap|md5chap> de config**

Remarque: Le serveur d'invité NAC utilise seulement le PAP.

Comment placer un invité de câble WLAN

Il est facile de configurer et très proche de la configuration Sans fil d'invité. Vous pouvez le configurer avec un ou deux contrôleurs (seulement si on est auto-ancrage).

Choisissez un VLAN comme VLAN dans lequel vous placez les utilisateurs de câble d'invité, par exemple, sur VLAN 50. Quand un invité de câble veut l'accès à Internet, branchez l'ordinateur portable à un port sur un commutateur configuré pour VLAN 50. Ce VLAN 50 doit être laissé et présent sur le chemin par le port de joncteur réseau WLC. Dans un cas de deux WLCs (une ancre et une étrangères), ce VLAN invité de câble doit mener au WLC étranger (WLC1 Désigné) et pas à l'ancre. WLC1 prend alors soin de percer un tunnel le trafic au DMZ WLC (l'ancre, WLC2 Désigné), qui libère le trafic dans le réseau routé.

Voici les cinq étapes pour configurer l'accès invité de câble :

1. **Configurez une interface dynamique (VLAN) pour l'accès client de câble d'invité.**

   Sur WLC1, créez une interface dynamique VLAN50. Dans la page de **configuration d'interface**, cochez la case de **RÉSEAU LOCAL d'invité**. Puis, les champs tels que l'**adresse IP** et la **passerelle** disparaissent. La seule chose que votre WLC doit savoir cette interface est que le trafic est conduit de VLAN 50. Ces clients sont les invités de câble.

2. **Créez un lan câblée pour l'accès client d'invité.**

   Sur un contrôleur, une interface est utilisée une fois associée à un WLAN. La deuxième étape est de créer un WLAN sur vos contrôleurs de bureau central. Naviguez vers des **WLAN** et cliquez sur New. Dans le **type WLAN**, choisissez le **RÉSEAU LOCAL d'invité**.

   Dans le **nom de profil** et le **WLAN SSID**, écrivez un nom qui identifie ce WLAN. Ces noms peuvent être différents, mais ne peuvent pas contenir les espaces. Le terme WLAN est utilisé, mais ce profil réseau n'est pas lié au profil réseau Sans fil.

   L'onglet Général offre deux listes déroulantes : **D'entrée** et **de sortie**. Le d'entrée est le VLAN dont les utilisateurs sont livré (VLAN 50) ; Le de sortie est le VLAN auquel vous voulez les envoyer.

   Pour le **d'entrée**, choisissez **VLAN50**.

   Pour le **de sortie**, il est différent. Si vous avez seulement un contrôleur, vous devez créer une autre interface dynamique, **standard** cette fois (pas un RÉSEAU LOCAL d'invité), et vous envoyez vos utilisateurs de câble à cette interface. Dans ce cas, envoyez-les au contrôleur DMZ. Par conséquent, pour l'**interface de sortie**, choisissez l'**interface de gestion**.

   La security mode pour ce RÉSEAU LOCAL « WLAN » d'invité est WebAuth, qui est acceptable. **Ok de** clic afin de valider.

3. **Configurez le contrôleur étranger (bureau central).**

   De la liste WLAN, cliquez sur l'**ancre de mobilité à l'**extrémité de la ligne de **RÉSEAU LOCAL d'invité**, et choisissez votre contrôleur DMZ. On le suppose ici que les deux contrôleurs se connaissent. S'ils ne se connaissent pas encore, allez au **contrôleur >** à la **gestion de la mobilité >** au **groupe de mobilité**, et ajoutez **DMZWLC** sur WLC1. Ajoutez alors **WLC1** sur DMZ. Les deux contrôleurs ne devraient pas être au même groupe de mobilité. Autrement, les règles de sécurité de base sont cassées.

4. **Configurez le contrôleur d'ancre (le contrôleur DMZ).**

   Votre contrôleur de bureau central est prêt. Vous devez maintenant préparer votre contrôleur DMZ. Ouvrez une session de navigateur Web à votre contrôleur DMZ et naviguez vers des **WLAN**. Créez un nouveau WLAN. Dans le **type WLAN**, choisissez le **RÉSEAU LOCAL d'invité**.

   Dans le **nom de profil** et le **WLAN SSID**, écrivez un nom qui identifie ce WLAN. Utilisez les mêmes valeurs qu'entrées sur le contrôleur de bureau central.

   L'interface d'entrée ici n'en est **aucune**. Il réellement n'importe pas, parce que le trafic est reçu par les Ethernets au-dessus du tunnel IP (EoIP). C'est pourquoi vous n'avez pas besoin de ne spécifier aucune interface d'entrée.

   L'interface de sortie est celle sur laquelle les clients sont censés être envoyés. Par exemple, le **VLAN DMZ** est VLAN 9. créent une interface dynamique standard pour VLAN 9 sur votre DMZWLC, puis choisissent **VLAN 9** comme interface de sortie.

   Vous devez configurer l'extrémité du tunnel d'ancre de mobilité. **De la liste WLAN**, choisissez l'**ancre de mobilité pour le RÉSEAU LOCAL d'invité**. Envoyez le trafic au contrôleur local, **DMZWLC**. Les deux buts sont maintenant prêts.

5. **Réglez avec précision le RÉSEAU LOCAL d'invité.**

   Vous pouvez également régler avec précision les configurations WLAN sur les deux extrémités. Faites attention, les configurations doit être identique sur les deux extrémités. Par exemple, si vous choisissez de cliquer sur dans l'**onglet Avancé WLAN**, **permettez le dépassement d'AAA** sur WLC1, vous doivent cocher la même case sur DMZWLC. S'il y a des différences dans les sélections dans le WLAN de chaque côté, le tunnel se casse. DMZWLC refuse le trafic ; vous pouvez voir quand vous **exécuter le debug mobility**.

   Maintenez dans l'esprit que toutes les valeurs sont obtenues réellement de DMZWLC : Adresses IP, valeurs VLAN, et ainsi de suite. Configurez le côté WLC1 identiquement, de sorte qu'il transmette par relais la demande au WLCDMZ.

Certificats pour la page de connexion

Cette section fournit les processus que vous devez suivre si vous voulez mettre votre propre

certificat sur la page de WebAuth, ou si vous voulez masquer l'URL de 1.1.1.1 WebAuth et afficher un URL Désigné.

Téléchargez un certificat pour l'authentification Web de contrôleur

Par le GUI (**WebAuth > certificat**) ou CLI (**webauthcert de** type de transfert) vous pouvez télécharger un certificat sur le contrôleur. Si c'est un certificat que vous avez créé avec votre Autorité de certification (CA) ou un tiers certificat officiel, il doit être dans le format .pem. Avant que vous envoyiez, vous devez également introduire la clé du certificat.

Après que le téléchargement, une réinitialisation soit exigé afin du certificat soit en place. Une fois que redémarré, allez à la page de certificat de WebAuth dans le GUI et il t'affiche les détails du certificat que vous avez téléchargé (validité et ainsi de suite). L'important champ est le nom commun (NC), qui est le nom fourni au certificat. Ce champ est discuté dans ce document sous la section « autorité de certification et d'autres Certificats sur le contrôleur ».

Après que vous ayez redémarré et ayez vérifié les détails du certificat, vous êtes présenté avec le nouveau certificat de contrôleur sur la page de connexion de WebAuth. Cependant, il peut y avoir deux situations.

1. Si votre certificat a été délivré par un des peu la racine principale CAs à la laquelle chaque ordinateur fait confiance, alors il est correct. Un exemple est Verisign, mais vous n'êtes habituellement signé par Verisign sous-titre-CA et pas la racine CA. Vous pouvez signer votre mémoire de certificat de navigateur si vous voyez le CA mentionné là comme fait confiance.

2. Si vous obteniez votre certificat d'un plus petit company/CA, tous les ordinateurs ne leur font pas confiance. Vous devriez fournir le certificat company/CA au client aussi bien, et si tout va bien un de la racine CAs délivrera ce certificat. Par la suite, vous finissez par avec une chaîne telle que le « certificat a été émis par CA X > certificat CA X a été émis par CA y > certificat CA y a été émis par ceci la racine de confiance CA ». L'objectif final est d'atteindre un CA au lequel le client fait confiance.

Autorité de certification et d'autres Certificats sur le contrôleur

Afin d'être débarrassé de l'avertissement que « ce certificat n'est pas fait confiance », vous doit également entrer dans le certificat du CA qui a délivré le certificat de contrôleur sur le contrôleur. Alors le contrôleur présente les deux Certificats (le certificat et son certificat de CA du contrôleur). Le certificat de CA devrait être un CA de confiance ou a les ressources pour vérifier le CA. Vous pouvez réellement construire une chaîne des Certificats CA qui mènent à un CA de confiance sur le dessus.

Vous devez placer la chaîne entière dans le même fichier. Ceci signifie que votre fichier contient le contenu tel que cet exemple :

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

Comment faire apparier le certificat l'URL

L'URL de WebAuth est placé à 1.1.1.1 afin de s'authentifier et le certificat est délivré (c'est le

champ NC du certificat WLC). Si vous voulez changer l'URL de WebAuth à « myWLC.com », par exemple, entrez dans la **configuration de** virtualinterface **(l'**interface de 1.1.1.1) et là vous pouvez entrer dans une **adresse Internet de** virtualDNS**, telle que** myWLC.com. Ceci remplace 1.1.1.1 dans votre barre URL. Ce nom doit également être résoluble. Le tracé de renifleur affiche comment cela tout fonctionne, mais quand WLC envoie la page de connexion, WLC affiche l'adresse de myWLC.com, et le client résout ce nom avec leurs DN. Ce nom devrait le résoudre comme 1.1.1.1. Ceci signifie que si vous utilisez également un nom pour la Gestion du WLC, vous devriez utiliser un nom différent pour WebAuth. En d'autres termes, si vous utilisez myWLC.com tracé à l'adresse IP de Gestion WLC, vous devez utiliser un nom différent pour le WebAuth, tel que myWLCwebauth.com.

Dépannez les questions de certificat

Cette section explique comment et ce qui à vérifier pour dépanner des questions de certificat.

Comment vérifier

Vous pouvez télécharger OpenSSL (pour Windows, rechercher OpenSSL Win32) et l'installer. Sans n'importe quelle configuration, vous pouvez entrer dans l'**openssl de** répertoire et d'essai de coffre **s_client – connectez** www.mywebauthpage.com:443, si cet URL est l'URL où votre page de WebAuth est jointe sur vos DN. Référez-vous à « ce que pour vérifier » la section de ce document pour un exemple.

Si vos Certificats utilisent un CA privé, vous devez placer le certificat de CA de racine dans un répertoire sur un ordinateur local et utiliser l'option d'openssl **- CApath**. Si vous avez une intermédiaire CA, vous devez la mettre dans le même répertoire aussi bien.

Afin d'obtenir les informations générales au sujet du certificat et les vérifier, utilisation :

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

Il pourrait être également utile de convertir des Certificats avec l'utilisation de l'openssl :

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

Ce qui à vérifier

Vous pouvez voir quels Certificats sont envoyés au client quand il se connecte. Lisez le certificat de périphérique — la NC devrait être l'URL où la page Web est accessible. Lisez « émis par » la ligne du certificat de périphérique. Ceci doit apparier la NC du deuxième certificat. Alors ce deuxième certificat « délivré par » doit apparier la NC du prochain certificat, et ainsi de suite. Autrement, il ne fait pas une vraie chaîne. Dans le résultat présenté d'OpenSSL ici, vous pouvez voir que l'**openssl** ne peut pas vérifier le certificat de périphérique parce que le son « émis par » n'apparie pas le nom du certificat de CA fourni.

Sortie 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)
---
```

Une autre question possible est le certificat ne peut pas être téléchargée au contrôleur. Dans cette situation il n'y a aucune question de validité, CA, et ainsi de suite. Afin de vérifier ceci, vous pouvez d'abord vérifier la Connectivité et l'essai de Protocole TFTP (Trivial File Transfer Protocol) pour transférer un fichier de configuration. Puis, si vous écrivez le **debug transfer toute la** commande d'**enable**, vous voyez que le problème est l'installation du certificat. Ceci a pu être dû à la clé fausse utilisée avec le certificat. Il pourrait également être que le certificat est dans un format faux ou est corrompu.

Cisco recommande que vous compariez le contenu de certificat à un certificat connu et valide. Ceci te permet pour voir si un attribut de **LocalkeyID** affiche tout le 0s (déjà produit). Si oui, alors le certificat devrait être reconverti. Il y a deux commandes avec OpenSSL qui te permettent pour retourner de .pem à .p12, et puis révise un .pem avec la clé de votre choix.

Pré-étape : Si vous receviez un .pem qui contient un certificat suivi d'une clé, copie/pâte la partie principale : **----COMMENCEZ LA CLÉ ---- jusqu'à ------- CLÉ DE FIN ------** du .pem dans « key.pem ».

1. **openssl pkcs12 - exportation - dans certificate.pem - inkey key.pem - newcert.p12 ?** Vous êtes incité avec une clé ; écrivez check123.

2. **l'openssl pkcs12 - dans newcert.p12 - workingnewcert.pem - le passin pass:check123 - le passout pass:check123 ceci** a comme conséquence un .pem opérationnel avec le mot de passe check123.

D'autres situations à dépanner

Bien que l'**ancre de mobilité** n'ait pas été discutée dans ce document, si vous êtes dans une situation **ancrée d'invité**, assurez-vous l'échange de mobilité se produit correctement et cela que vous voyez que le client arrive sur l'ancre. Tout autre besoin de problèmes de WebAuth dépannent sur l'ancre.

Voici quelques problèmes courants que vous pouvez dépanner :

- **Les utilisateurs ne peuvent pas s'associer au WLAN invité**.

  Ceci n'est pas lié à WebAuth. Vérifiez la configuration de client, les paramètres de sécurité sur le WLAN, s'il est activé, et si les radios sont en activité et en état de fonctionnement, et ainsi de suite.

- **Les utilisateurs n'obtiennent pas l'adresse IP**.

  Dans une situation d'ancre d'invité, c'est le plus souvent parce que l'étranger et l'ancre n'ont pas été configurés exactement la même manière. Autrement, vérifiez la configuration DHCP, Connectivité, et ainsi de suite. Confirmez si d'autres WLAN peuvent utiliser le même serveur DHCP sans problème. Ceci n'est toujours pas lié à WebAuth.

- **L'utilisateur n'est pas réorienté à la page de connexion**.

  C'est la plupart de symptôme commun, mais est plus précis. Il y a deux scénarios possibles.

  L'utilisateur n'est pas réorienté (l'utilisateur écrit un URL et n'atteint jamais la page de WebAuth). Pour cette situation, contrôle :

  qu'un serveur DNS valide a été assigné au client par l'intermédiaire de DHCP (**ipconfig /all**),

  que les DN est accessible du client (**nslookup** www.website.com),

  que l'utilisateur est entré dans un URL valide afin de pour être réorienté,

  que l'utilisateur est allé sur un URL HTTP sur le port 80 (par exemple, pour atteindre un ACS avec http://localhost:2002 ne vous réoriente pas puisque vous avez envoyé en fonction le port 2002 au lieu de 80).

  L'utilisateur est réorienté à 1.1.1.1 correctement, mais la page elle-même n'affiche pas.

  Cette situation est le plus susceptible un problème WLC (bogue) ou un problème de côté client. Il pourrait être que le client a un certain Pare-feu ou logiciel ou stratégie de blocage. Il pourrait également être qu'ils ont configuré un proxy en leur navigateur Web.

  Recommandation : Prenez un tracé de renifleur sur le PC client. Il n'y a aucun besoin de logiciel Sans fil spécial, seulement Wireshark, qui fonctionne sur l'adaptateur Sans fil et t'affiche si le WLC répond et essaye pour réorienter. Vous avez deux possibilités : ou il n'y a

aucune réponse de WLC, ou quelque chose est erronée avec la prise de contact SSL pour la page de WebAuth. Pour la question de prise de contact SSL, vous pouvez vérifier si le navigateur d'utilisateur tient compte de SSLv3 (certains permettent seulement SSLv2), et s'il est trop agressif sur la vérification de certificat.

C'est une étape commune pour entrer dans manuellement http://1.1.1.1 afin de vérifier si la page Web paraît sans DN. En fait, vous pouvez taper http://6.6.6.6 et obtenir le même effet. Le WLC réoriente n'importe quelle adresse IP que vous écrivez. Par conséquent, si vous entrez dans http://1.1.1.1, il ne vous fait pas fonctionner autour de la redirection de Web. Si vous entrez dans https://1.1.1.1 (sécurisez), ceci ne fonctionne pas parce que WLC ne réoriente pas le trafic HTTPS (par défaut, c'est réellement possible dans la version 8.0 et ultérieures). La meilleure manière de charger la page directement sans réorientation est d'entrer dans https://1.1.1.1/login.html.

- **Les utilisateurs ne peuvent pas authentifier**.

  Voyez la section de ce document qui discute l'authentification. Qualifications de contrôle localement sur le RAYON.

- **Les utilisateurs peuvent avec succès authentifier par WebAuth, mais ils n'ont pas accès d'Internet après**.

  Vous pouvez retirer WebAuth de la Sécurité du WLAN, et alors vous devriez avoir un WLAN ouvert. Vous pouvez alors essayer d'accéder au Web, les DN et ainsi de suite. Si vous éprouvez des questions là aussi bien, retirez les configurations de WebAuth totalement et vérifiez votre configuration d'interfaces.

Pour plus d'informations à ce sujet, consultez : Dépannage de l'authentification Web sur un contrôleur LAN Sans fil (WLC).

Serveur proxy de HTTP et comment cela fonctionne

Vous pouvez utiliser un serveur proxy de HTTP. Si vous avez besoin du client pour ajouter une exception en son navigateur que 1.1.1.1 n'est pas de passer par le serveur proxy, vous pouvez faire le WLC écouter le trafic http sur le port du serveur proxy (habituellement 8080).

Afin de comprendre ce scénario, vous devez savoir ce qu'un proxy HTTP fait. Il est quelque chose que vous configurez sur le côté client (adresse IP et port) dans le navigateur.

Le scénario habituel quand un utilisateur visite un site Web est de résoudre le nom à l'IP avec des DN, et alors lui demande la page Web au web server. Le processus devrait toujours envoyer la demande de HTTP de la page au proxy. Le proxy traite les DN, s'il y a lieu, et en avant au web server (si la page n'est pas déjà cachée sur le proxy). La discussion est client-à-proxy seulement. Si le proxy obtient la vraie page Web est inutile au client.

Voici le procédé d'authentification Web :

- L'utilisateur saisit un URL.
- Le PC client envoie au serveur proxy.

- WLC intercepte et charrie l'IP de serveur proxy ; il répond au PC avec un redirect to 1.1.1.1.

Àce stade, si le PC n'est pas configuré pour lui, il demande la page de 1.1.1.1 WebAuth au proxy ainsi cela ne fonctionne pas. Le PC doit faire une exception pour 1.1.1.1 ; alors il envoie une demande de HTTP à 1.1.1.1 et se poursuit par WebAuth. Une fois authentifiées, toutes les transmissions passent par le proxy de nouveau. Une configuration d'exception est habituellement dans le navigateur près de la configuration du serveur proxy. Vous devriez voir le message : « N'utilisez pas le proxy pour ces adresses IP ».

Avec la version 7.0 et ultérieures WLC, le **proxy de webauth de** caractéristique **réorientent** peut être activé dans les options de configuration globales WLC. Une fois activé, le WLC vérifie si les clients sont configurés pour utiliser manuellement un proxy. Dans ce cas, ils réorientent le client à une page qui leur affiche comment modifier leurs paramètres de proxy pour faire fonctionner tout. Le proxy de WebAuth réorientent peut être configuré pour travailler à un grand choix de ports et est compatible avec l'authentification Web centrale.

Pour un exemple sur la redirection de proxy de WebAuth, référez-vous au proxy d'authentification Web sur un exemple Sans fil de configuration de contrôleur LAN.

Authentification Web sur le HTTP au lieu de HTTPS

Vous pouvez ouvrir une session sur l'authentification Web sur le HTTP au lieu de HTTPS. Si vous ouvrez une session sur le HTTP, vous ne recevez pas des alertes de certificat.

Pour plus tôt que le code de version 7.2 WLC, vous devez désactiver la Gestion HTTPS du WLC et laisser la Gestion de HTTP. Cependant, ceci permet seulement la Gestion de Web du WLC au-dessus du HTTP.

Pour le code de version 7.2 WLC, utilisez la commande de **débronchement de secureweb de Web-auth de réseau de config** de désactiver. Ceci désactive seulement HTTPS pour l'authentification Web et pas la Gestion. Notez que ceci exige une réinitialisation du contrôleur !

Sur le code de version 7.3 et ultérieures WLC, vous pouvez activer/HTTPS pour WebAuth seulement par l'intermédiaire du GUI et du CLI.

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Logiciel de téléchargement pour des paquets de WebAuth de contrôleur sans-fil
- Création d'une page de connexion personnalisée d'authentification Web
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Exemple de configuration du transit Web sur un contrôleur de réseau local sans fil
- Utilisant le GUI pour configurer le Web réorientez
- Utilisant le CLI pour configurer le Web réorientez
- Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil
- Proxy d'authentification Web sur un exemple Sans fil de configuration de contrôleur LAN
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems