Contenu

Introduction

Ce document comporte des informations sur les questions les plus souvent posées (FAQ) au sujet de la fonctionnalité d'accès invité sans fil, qui intègre le réseau sans fil unifié Cisco.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Q. Qu'est-ce qu'un tunnel Ethernet sur IP (EoIP) vers une zone de réseau non sécurisé ?

A. Cisco recommande l'utilisation d'un contrôleur dédié au trafic invité. Ce contrôleur est connu comme contrôleur d'ancrage invité.

Le contrôleur d'ancrage invité est habituellement situé dans une zone de réseau non sécurisé, souvent appelée la zone démilitarisée (DMZ). D'autres contrôleurs WLAN internes se trouvant où le trafic est généré se situent dans le réseau local de l'entreprise. Un tunnel EoIP est établi entre les contrôleurs WLAN internes et le contrôleur d'ancrage invité afin d'assurer l'isolement du chemin du trafic invité vis-à-vis du trafic de données de l'entreprise. L'isolement du chemin est une fonctionnalité essentielle de la gestion de la sécurité pour l'accès invité. Il assure que les politiques de sécurité et de qualité de service (QoS) puissent être distinctes et différenciées entre le trafic des invités et le trafic de l'entreprise ou interne.

Une importante fonctionnalité de l'architecture du réseau sans fil unifié Cisco est la capacité d'utiliser un tunnel EoIP pour mapper statiquement un ou plusieurs WLAN équipés (c'est-à-dire, des SSID) vers un contrôleur spécifique d'ancrage invité dans le réseau. Tous trafiquent ? chacun des deux à et d'un WLAN tracé ? traverse un tunnel statique d'EoIP qui est établi entre un contrôleur distant et le contrôleur d'ancre d'invité.

Àl'aide de cette technique, tout le trafic invité associé peut être transporté d'une manière transparente à travers le réseau de l'entreprise vers un contrôleur d'ancrage invité qui réside dans la zone de réseau non sécurisé.

Q. Comment est-ce que je sélectionne le contrôleur correct à déployer comme contrôleur d'ancrage invité ?

A. La sélection du contrôleur d'ancrage invité constitue une fonction du volume du trafic invité tel que défini par le nombre de sessions actives de clients invités ou tel que défini par la capacité d'interface de la liaison ascendante sur le contrôleur, ou les deux.

Les limites de débit total et de clients par contrôleur d'ancrage invité sont les suivantes :

- Contrôleur LAN de radio de Cisco 2504 ? interfaces 4 * 1 GBP et 1000 clients d'invité

- Contrôleur LAN Sans fil de Cisco 5508 (WLC) ? 8 GBP et 7,000 clients d'invité
- Wireless Services Module de gamme Cisco Catalyst 6500 (WiSM-2) ? 20 GBP et 15,000 clients
- Contrôleur LAN Sans fil de Cisco 8500 (WLC) ? 10 Gbits/s et 64,000 clients

Remarque: Le Cisco 7500 WLCs ne peut pas être configuré comme contrôleur d'ancre d'invité. Référez-vous quels contrôleurs peuvent être utilisés pour prendre en charge l'accès invité dans la zone de réseau non sécurisé ? pour la liste de WLCs qui prennent en charge la fonction d'ancre d'invité.

Un maximum de 2048 noms d'utilisateur et mot de passe d'invité peut être enregistré sur chaque contrôleur ? base de données s. Par conséquent, si le nombre total d'informations d'identification d'invités actifs est inférieur à ce nombre, plusieurs contrôleurs seront nécessaires. En alternative, les informations d'identification d'invités peuvent être enregistrées dans un serveur RADIUS externe.

Le nombre de points d'accès dans le réseau n'affecte pas la sélection du contrôleur d'ancrage invité.

Q. Combien de tunnels Ethernet sur IP (EoIP) peuvent-ils être terminés sur un contrôleur d'ancrage d'invités ?

A. Un contrôleur d'ancrage invité peut terminer jusqu'à 71 tunnels EoIP à partir des contrôleurs WLAN internes. Cette capacité est identique à travers n'importe quel modèle du contrôleur LAN Sans fil de Cisco excepté WLC- 2504. Le contrôleur 2504 peut terminer jusqu'à 15 tunnels d'EoIP. Plusieurs contrôleurs d'ancrage invité peuvent être configurés si des tunnels supplémentaires sont requis.

Des tunnels EoIP sont comptés par contrôleur WLAN, indépendamment du nombre de WLAN tunnelisés ou de SSID (Secure Set Identifiers) dans chaque EoIP.

Un tunnel EoIP est configuré entre le contrôleur d'ancrage invité et chaque contrôleur interne qui prend en charge des points d'accès avec des associations de clients invités.

Q. Est-ce que je peux créer des tunnels Ethernet sur IP (EoIP) entre des contrôleurs qui exécutent différentes versions du logiciel ?

A. Les versions du logiciel du contrôleur de réseau local sans fil ne le prennent pas toutes en charge. Dans ces cas, le contrôleur d'ancrage et distant devrait exécuter la même version du logiciel WLC. Cependant, les récentes versions du logiciel permettent aux contrôleurs d'ancrage et distants d'avoir différentes versions.

Cette matrice énumère les versions du logiciel du contrôleur de réseau local sans fil avec lesquelles vous pouvez créer les tunnels EoIP.

EoIP Tunnel Combination Between WLC Versions

Anchor / Remote	4.1.185	4.2.X	5.0.X	5.1.X	5.2.X	6.0.X	7.0.X
4.1.185	✓						
4.2.X		✓		✓	✓	✓	✓
5.0.X			✓	✓	✓	✓	✓
5.1.X		✓	✓	✓	✓	✓	✓
6.0.X		✓	✓	✓	✓	✓	✓
7.0.X		✓	✓	✓	✓	✓	✓

4.2.x = 4.2.61.0, 4.2.99.0, 4.2.112.0, 4.2.130.0, 4.2.173.0, 4.2.176.0, 4.2.205.0, 4.2.207.0, 4.2.209.0
5.0.x = 5.0.148.0, 5.0.148.2
5.1.x = 5.1.151.0, 5.1.163.0
5.2.x = 5.2.157.0, 5.2.178.0, 5.2.193.0
6.0.X = 6.0.182.0, 6.0.188.0, 6.0.190.0, 6.0.199.0, 6.0.202.0
7.0.X = 7.0.98.0, 7.0.116.0 , 7.0.220.0

Q. Le contrôleur LAN Sans fil de gamme Cisco 2100/2500 peut-il être utilisé comme contrôleur d'ancre d'invité dans la zone de réseau non sécurisé ?

A. Oui, démarrant la version de logiciel 7.4 de réseau sans fil unifié Cisco, le contrôleur LAN Sans fil de gamme Cisco 2500 peut terminer le trafic d'invité (de jusqu'à 15 tunnels d'EoIP) en dehors du Pare-feu. Le contrôleur de réseau local sans fil de la gamme Cisco 2000 peut seulement initier des tunnels d'invités.

Q. Le module du contrôleur LAN sans fil pour des Integrated Services Router (WLCM ou WLCM2) peut-il être utilisé comme contrôleur d'ancre d'invité dans la zone de réseau non sécurisé ?

A. Non, le WLCM ou WLCM2 ne peuvent pas terminer des tunnels d'invité. Le WLCM peut seulement initier des tunnels d'invités.

Q. Quels contrôleurs peuvent-ils être utilisés pour prendre en charge l'accès invité dans la zone de réseau non sécurisé ?

A. La fonction d'ancre de tunnel d'invité, qui inclut l'arrêt, l'authentification Web, et le contrôle d'accès de tunnel d'EoIP des clients d'invité, est prise en charge dans des ces Plateformes Sans fil de contrôleur LAN de Cisco avec des images logicielles de version 4.0 ou ultérieures :

- Wireless Services Module de gamme Cisco Catalyst 6500 (WiSM2)
- Contrôleur LAN de radio de gamme de Cisco WiSM-2
- Contrôleur de réseau local sans fil intégré Cisco Catalyst 3750G
- Contrôleur LAN de radio de gamme Cisco 5508
- Contrôleur LAN Sans fil de gamme Cisco 2500 (support introduit dans la version de logiciel 7.4)

Q. Si un contrôleur d'ancrage invité est utilisé en dehors du pare-feu, quels ports de pare-feu sont-ils ouverts pour que l'accès invité fonctionne ?

A. Sur n'importe quel pare-feu entre le contrôleur d'ancrage invité et les contrôleurs distants, ces ports doivent être ouverts :

- Protocole IP 97 pour le trafic de données de l'utilisateur
- Port UDP pour le trafic de contrôle de tunnel

Pour la gestion facultative, ces ports de pare-feu doivent être ouverts :

- SSH/Telnet ? Port TCP 22/23
- TFTP ? Port UDP 69
- NTP ? Port UDP 123
- SNMP ? Ports UDP 161 (obtient et place) et 162 (déroutements)
- HTTPS/HTTP ? Port TCP 443/80
- Syslog ? Port TCP 514
- RAYON authentique/port UDP 1812 et 1813 de compte

Q. Le trafic invité peut-il passer à travers un pare-feu lorsque la traduction

d'adresses réseau (NAT) est configurée ?

A. Une NAT linéaire doit être utilisée sur le tunnel EoIP passant à travers un pare-feu.

Q. Dans un scénario ancrage - WLC étranger, quel WLC envoie-t-il la gestion des comptes RADIUS ?

A. Dans ce scénario, l'authentification est toujours effectuée par l'ancrage WLC. Par conséquent, la gestion des comptes de RADIUS est envoyée par l'ancrage WLC.

Q. Le tunnel des invités entre le contrôleur interne et le contrôleur d'ancrage échoue. Je vois ces messages dans le WLC : `mm_listen.c:5373 MM-3-INVALID_PKT_RECVD : A reçu un paquet incorrect de 10. 40.220.18.` Source member:0.0.0.0. source member unknown... Pourquoi ?

A. Vous vérifiez l'état du tunnel à partir de la GUI du WLC sur la page des **WLAN**. Cliquez sur la liste déroulante près d'un WLAN et choisissez **Ancres de mobilité** , où figure l'état du contrôle et le chemin des données. Le message d'erreur s'affiche pour l'une des raisons suivantes :

1. Les contrôleurs d'ancrage et internes se trouvent sur différentes versions de code. Assurez-vous qu'ils exécutent les mêmes versions du code.
2. Configurations incorrectes dans la configuration de l'ancre de mobilité. Vérifiez que le DMZ est lui-même configuré en tant qu'ancre de mobilité et que les WLC internes ont le DMZ WLC configuré en tant qu'ancre de mobilité. Pour plus d'informations sur la façon configurer l'ancre de mobilité, référez-vous à la section de configuration de mobilité d'auto-ancrage du guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0. En conséquence, les utilisateurs invités ne seraient pas en mesure de transmettre le trafic.

Q. Dans une installation d'accès invité sans fil, les clients ne reçoivent pas l'adresse IP du serveur DHCP. Thu le 22 janvier 16:39:09 2009 : XX : XX : XX : XX : XX : XX LA RÉPONSE chutante DHCP du message d'erreur Exportation- apparaît sur le contrôleur interne. Pourquoi ?

A. Dans une installation d'accès invité sans fil, le paramètre de proxy DHCP dans les contrôleurs d'ancre d'invité et le contrôleur interne doivent s'assortir. Autrement, la requête DHCP des clients sont abandonnées et vous voyez ce message d'erreur sur le contrôleur interne :

Employez cette commande afin de changer le paramètre de proxy DHCP sur le WLC :

```
(Cisco Controller) >config dhcp proxy ?enable         Enable DHCP processing's proxy style behaviour.disable        Disable DHCP processing's proxy style behaviour.
```

Employez la commande de **show dhcp proxy** sur les deux contrôleurs afin de vérifier que les deux contrôleurs ont le même paramètre de proxy DHCP.

```
(Cisco Controller) >show dhcp proxyDHCP Proxy Behaviour: enabled(Cisco Controller) >
```

Q. Si le trafic invité est tunnelisé vers une zone de réseau non sécurisé, où les clients invités obtiennent-ils une adresse IP ?

A. Le trafic invité est transporté au sein de l'entreprise à la couche 3 via EoIP. Par conséquent, le

premier point sur lequel les services de protocole de configuration dynamique d'hôte (DHCP) peuvent être mis en application réside au niveau local, sur le contrôleur d'ancrage invité. Le contrôleur d'ancrage invité peut également relayer des requêtes DHCP de clients vers un serveur externe. Il s'agit également de la méthode à travers laquelle la résolution d'adresse du système de noms de domaine (DNS) est prise en charge.

Q. Le contrôleur de réseau local sans fil Cisco prend-il en charge des portails Web pour l'authentification des invités ?

A. Les contrôleurs de réseau local sans fil Cisco (version 3.2 ou ultérieure) fournissent un portail Web intégré qui saisit les informations d'identification d'invités en vue de leur authentification et offre des fonctionnalités de marquage simple, conjointement avec la capacité d'afficher l'avis de non-responsabilité ainsi que la politique d'utilisation acceptable.

Q. Comment puis-je personnaliser le portail Web ?

A. Pour les informations relatives à la façon de personnaliser un portail Web, reportez-vous à Choisir la page de connexion d'authentification Web.

Q. Comment les informations d'identification des invités sont-elles gérées ?

A. Des qualifications d'invité peuvent être créées et gérées centralement utilisant la version 7.0 du Système de contrôle sans fil Cisco (WCS) et ou le ver 1.0 du Système de contrôle de réseau (NCS). Un administrateur réseau peut établir un compte administratif de limité-privilège dans WCS qui laisse ? ambassadeur de lobby ? accès afin de créer des qualifications d'invité. Dans WCS ou NCS, la personne avec un compte d'ambassadeur de lobby peut créer, assigner, surveiller, et supprimer l'invité les qualifications pour le service de contrôleur en tant qu'invité ancrent le contrôleur.

Le « lobby ambassador » peut entrer le nom de l'utilisateur invité (ou ID utilisateur) et le mot de passe, les informations d'identification pouvant également être autogénérées. Il y a également un paramètre de configuration globale qui permet l'utilisation d'un nom d'utilisateur et d'un mot de passe pour tous les invités, ou un seul nom d'utilisateur et mot de passe pour chaque invité.

Afin de configurer le compte d'ambassadeur de lobby sur le WCS, référez-vous à la section de création de comptes d'utilisateur d'invité du guide de configuration de Système de contrôle sans fil Cisco, version 7.0.

Q. La fonction d'ambassadeur de lobby disponible à Cisco contrôleur LAN est-elle Sans fil en plus du système de contrôle sans fil (WCS) ou de NCS ?

A. Oui. Si le WCS ou le NCS n'est pas déployé, un administrateur réseau peut établir un compte d'ambassadeur de lobby sur le contrôleur d'ancre d'invité. Une personne qui se connecte au contrôleur d'ancrage invité en utilisant le compte « lobby ambassador » aura seulement accès aux fonctions de gestion d'utilisateur invité.

S'il y a de plusieurs contrôleurs d'ancre d'invité, un WCS ou un NCS doit être utilisé pour configurer simultanément des noms d'utilisateur sur de plusieurs contrôleurs d'ancre d'invité.

Pour les informations sur la façon dont créer des comptes d'ambassadeur de lobby utilisant les contrôleurs LAN Sans fil, référez-vous à créer une section de l'Ambassadeur Account de lobby de

guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0.

Q. Les invités peuvent-ils être authentifiés à travers une authentification externe, une autorisation et un serveur de gestion des comptes (AAA) ?

A. Oui. Des demandes d'authentification d'invités peuvent être relayées vers un serveur RADIUS externe.

Q. Que se produit-il quand un invité ouvre une session ?

A. Quand un invité sans fil se connecte à travers le portail Web, le contrôleur d'ancrage invité prend en charge l'authentification en effectuant ces étapes :

1. Le contrôleur d'ancrage invité vérifie la présence du nom d'utilisateur et du mot de passe dans sa base de données locale et, le cas échéant, accorde l'accès.
2. Si aucune information d'identification des utilisateurs n'est présente localement sur le contrôleur d'ancrage invité, le contrôleur d'ancrage invité vérifie des paramètres de configuration WLAN pour déterminer si un ou plusieurs serveurs externes de RADIUS ont été configurés pour le WLAN invité. Le cas échéant, le contrôleur crée un paquet de demande d'accès RADIUS avec le nom d'utilisateur et le mot de passe et le transfère au serveur RADIUS sélectionné pour l'authentification.
3. Si aucun serveur RADIUS spécifique n'a été configuré pour le WLAN, le contrôleur vérifie les paramètres de configuration globale du serveur RADIUS. Des serveurs RADIUS externes configurés avec l'option d'authentifier ? utilisateur du réseau ? sera questionné avec l'utilisateur d'invité ? qualifications s. Autrement, si aucun serveur n'a ? utilisateur du réseau ? sélectionné, et l'utilisateur n'a pas été authentifié par les étapes 1 ou 2, l'authentification échouera.

Q. Est-il possible d'ignorer l'authentification de l'utilisateur invité et de n'afficher que l'option d'avis de non-responsabilité de la page Web ?

A. Oui. Une autre option de configuration d'accès invité sans fil est de contourner totalement l'authentification des utilisateurs et de permettre un accès ouvert. Cependant, il pourrait être nécessaire de présenter une page de politique d'utilisation acceptable et d'avis de non-responsabilité aux invités avant de leur concéder l'accès. À cette fin, un WLAN invité peut être configuré pour le passthrough de la politique Web. Dans ce scénario, un utilisateur invité est redirigé vers une page de portail Web qui contient les informations d'avis de non-responsabilité. Afin de permettre l'identification de l'utilisateur invité, le mode passthrough a également une option pour qu'un utilisateur entre une adresse e-mail avant de se connecter.

Q. Est-il nécessaire que le contrôleur distant et le contrôleur d'ancrage invité se trouvent dans le même groupe de mobilité ?

A. Non. Le contrôleur d'ancrage invité et le contrôleur distant peuvent se trouver dans des groupes de mobilité distincts.

Q. En présence de plus d'un SSID invité, chaque WLAN (SSID) peut-il être dirigé vers un seul portail de page Web ?

A. Oui. Tout le trafic invité, sur un ou plusieurs WLAN, sont redirigés vers une page Web. À partir de la version 4.2 ou ultérieure de WLC, chaque WLAN peut être dirigé vers une seule page du portail Web. Référez-vous à la procédure de connexion, à la panne de procédure de connexion, et aux pages assignantes de déconnexion par section WLAN de guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0.

Q. Quelle est la fonctionnalité du nouveau paramètre dans la version 7.0 WLC, WebAuth sur la panne de filtre de MAC ?

A. Si un WLAN a une couche 2 (MAC-filtre) et pose la Sécurité 3 (webauth-sur-macfilter-panne) configurée, le client se déplace à l'état de PASSAGE si l'un ou l'autre un est passé. Et s'il échoue degré de sécurité de la couche 2 (MAC-filtre), le client est déplacé pour poser la Sécurité 3 (webauth-sur-macfilter-panne).

Q. Le client fonctionne-t-il correctement si le navigateur est configuré pour le serveur proxy ?

A. Avant la version 7.0, le client ne pourrait pas établir une connexion TCP quand le serveur proxy a été configuré dans le programme de lecture. Après version 7.0, ce support de serveur proxy de WebAuth est ajouté et l'IP address et le port de serveur proxy peuvent être configurés sur le contrôleur.

Q. Existe-t-il un guide de déploiement pour l'accès invité sans fil ?

A. Voici le lien au guide de déploiement :

Guide de déploiement : Accès invité de Cisco en utilisant le contrôleur de réseau local sans fil Cisco

Q. Existe-t-il un guide de conception pour l'accès invité sans fil ou câblé ?

A. Voici le lien aux guides de conception :

Services d'accès invité de Cisco sans fil unifié

Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco

Informations connexes

- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco
- Guide de déploiement : Accès invité de Cisco utilisant le contrôleur de réseau local sans fil Cisco, version 4.1
- Support et documentation techniques - Cisco Systems