Matrice de compatibilité du contrôleur de réseau local sans fil avec sécurité de couche 2 et 3

Contenu

Introduction

Ce document fournit la matrice de compatibilité pour les mécanismes de sécurité de la couche 2 et de la couche 3 pris en charge sur le contrôleur LAN Sans fil (WLC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration des AP légers et des WLC de Cisco
- Avoir une connaissance de base du protocole LWAPP (Lightweight AP Protocol)
- Connaissance de base des solutions de sécurité sans fil

Composants utilisés

Les informations dans ce document sont basées sur une gamme Cisco 4400/2100 WLC qui exécutent la version 7.0.116.0 de micrologiciels

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.

Conventions

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

Solutions de sécurité de réseau sans fil unifié Cisco

Les supports de réseau sans fil unifié Cisco posent 2 et posent 3 méthodes de Sécurité.

- Degré de sécurité de la couche 2
- Degré de sécurité de la couche 3 (pour le WLAN) ou degré de sécurité de la couche 3 (pour le RÉSEAU LOCAL d'invité)

Le degré de sécurité de la couche 2 n'est pas pris en charge sur des réseaux locaux d'invité.

Cette table des méthodes cote diverses de la couche 2 et de la couche 3 valeurs mobilières prises en charge sur le contrôleur LAN Sans fil. Ces méthodes de Sécurité peuvent être activées de l'**onglet Sécurité à la** page de **WLANs > Edit du** WLAN.

Mécanisme de sécurité de la couche 2		
Paramètre		**Description**
Degré de sécurité de la couche 2	Aucune	Aucun degré de sécurité de la couche 2 sélectionné.
	WPA+WPA2	Utilisez ce établissement afin d'activer l'accès protégé par Wi-Fi.
	802.1X	Utilisez ce établissement afin d'activer l'authentification de 802.1x.
	WEP statique	Utilisez ce établissement afin d'activer le cryptage WEP statique.
	Statique WEP + 802.1x	Utilisez ce établissement afin d'activer des paramètres statiques WEP et de 802.1x.
	CKIP	Utilisez ce établissement afin d'activer le Cisco Key Integrity Protocol (CKIP). Fonctionnel sur AP modèle 1100, 1130, et 1200, mais pas AP 1000. L'élément d'information Aironet doit être activé pour que cette fonctionnalité fonctionne. CKIP développe les clés de chiffrement à 16 octets.
Filtrage MAC	Sélectionnez pour filtrer des clients par l'adresse MAC. Configurez localement les clients par l'adresse MAC dans les filtres d'adresses MAC > nouvelle page. Autrement, configurez les clients sur un serveur de	

	RADIUS.	
Mécanisme de sécurité de la couche 3 (pour le WLAN)		
Paramètre		**Description**
Degré de sécurité de la couche 3	Aucune	Aucun degré de sécurité de la couche 3 sélectionné.
	IPsec	Utilisez ce établissement afin d'activer IPSec. Vous devez vérifier la disponibilité logicielle et la compatibilité de matériel client avant que vous implémentiez IPSec. **Remarque:** Vous devez faire installer le module facultatif de Sécurité VPN/Enhanced (crypto carte processeur) pour activer IPSec. Vérifiez-le est installé sur votre contrôleur à la page d'inventaire.
	Intercommunication VPN	Utilisez ce établissement afin d'activer l'intercommunication VPN. **Remarque:** Cette option n'est pas disponible sur des contrôleurs de gamme Cisco 5500 et des contrôleurs de gamme Cisco 2100. Cependant, vous pouvez répliquer cette fonctionnalité sur une gamme Cisco 5500 contrôleur ou le contrôleur de gamme Cisco 2100 en créant un WLAN ouvert utilisant un ACL.
Stratégie de Web	Sélectionnez cette case pour activer la stratégie de Web. De contrôleur le trafic DNS en avant à et des clients sans fil avant l'authentification. **Remarque:** La stratégie de Web ne peut pas être utilisée en combination avec des options d'IPsec ou d'intercommunication VPN. Ces paramètres sont affichés : • Authentification — Si vous sélectionnez cette option, l'utilisateur est incité pour le nom d'utilisateur et mot de passe tout en connectant le client au réseau Sans fil. • Fonction émulation — Si vous sélectionnez cette option, l'utilisateur peut	

	accéder au réseau directement sans authentification de nom d'utilisateur et mot de passe. • Le Web conditionnel réorientent — Si vous sélectionnez cette option, l'utilisateur peut être conditionnellement réorienté à une page Web particulière après que l'authentification de 802.1X se termine avec succès. Vous pouvez spécifier la page de redirection et les conditions sous lesquelles celle-ci se produit sur votre serveur RADIUS. • Le Web de page de splash réorientent — Si vous sélectionnez cette option, l'utilisateur est réorienté à une page Web particulière après que l'authentification de 802.1X se termine avec succès. Après que la réorientation, l'utilisateur ait l'accès complet au réseau. Vous pouvez spécifier la page Web de splash sur votre serveur de RADIUS. • Sur la panne de filtre d'adresses MAC — Active des pannes de filtre d'adresses MAC d'authentification Web.
ACL de Préauthentification	Sélectionnez l'ACL à utiliser pour le trafic entre le client et le contrôleur.
Configuration globale de priorité	Affichages si vous sélectionnez l'authentification. Cochez cette case afin d'ignorer la définition de configuration globale d'authentification sur la page Web Login.
Type authentique de Web	Affichages si vous sélectionnez la stratégie de Web et ignorez la configuration globale. Sélectionnez un type d'authentification Web : • **Interne** • Personnalisé (téléchargé) Page de connexion — Sélectionnez une page de connexion de la liste déroulante.Page de panne de procédure de connexion — Sélectionnez une page de connexion qui affiche au client si l'authentification Web échoue.Page de déconnexion — Sélectionnez une page de connexion qui affiche au client quand les journaux de l'utilisateur hors du système. • Externe (réorientez au serveur externe)

<table>
<tr><td></td><td colspan="2">URL — Écrivez l'URL du serveur externe.</td></tr>
<tr><td>Entrée d'email</td><td colspan="2">Affichages si vous sélectionnez la fonction émulation. Si vous sélectionnez cette option, vous êtes incité pour votre adresse e-mail tout en se connectant au réseau.</td></tr>
<tr><td colspan="3">Mécanisme de sécurité de la couche 3 (pour le RÉSEAU LOCAL d'invité)</td></tr>
<tr><td colspan="2">Paramètre</td><td>Description</td></tr>
<tr><td rowspan="3">Degré de sécurité de la couche 3</td><td>Aucune</td><td>Aucun degré de sécurité de la couche 3 sélectionné.</td></tr>
<tr><td>Authentification Web</td><td>Si vous sélectionnez cette option, vous êtes incité pour le nom d'utilisateur et mot de passe tout en connectant le client au réseau.</td></tr>
<tr><td>Fonction émulation de Web</td><td>Si vous sélectionnez cette option, vous pouvez accéder au réseau directement sans authentification de nom d'utilisateur et mot de passe.</td></tr>
<tr><td colspan="2">ACL de Préauthentification</td><td>Sélectionnez l'ACL à utiliser pour le trafic entre le client et le contrôleur.</td></tr>
<tr><td colspan="2">Configuration globale de priorité</td><td>Cochez cette case afin d'ignorer la définition de configuration globale d'authentification sur la page Web Login.</td></tr>
<tr><td colspan="2">Type authentique de Web</td><td>Affichages si vous sélectionnez la configuration globale de priorité. Sélectionnez un type d'authentification Web :
Interne
Personnalisé (téléchargé) Page de connexion — Sélectionnez une page de connexion de la liste déroulante.Page de panne de procédure de connexion — Sélectionnez une page de connexion qui affiche au client si</td></tr>
</table>

	l'authentification Web échoue.Page de déconnexion — Sélectionnez une page de connexion qui affiche au client quand les journaux de l'utilisateur hors du système. • Externe (réorientez au serveur externe) URL — Écrivez l'URL du serveur externe.
Entrée d'email	Affichages si vous sélectionnez la fonction émulation de Web. Si vous sélectionnez cette option, vous êtes incité pour votre adresse e-mail tout en se connectant au réseau.

Remarque: Dans la version de logiciel de logiciel contrôleur 4.1.185.0 ou plus tard, CKIP est prise en charge pour l'usage seulement avec le WEP statique. Il n'est pas pris en charge pour l'usage avec le WEP dynamique. Par conséquent, un client sans fil qui est configuré pour utiliser CKIP avec le WEP dynamique ne peut pas s'associer à un RÉSEAU LOCAL Sans fil qui est configuré pour CKIP. Cisco recommande que vous utilisiez le WEP dynamique sans CKIP (qui est moins sécurisé) ou WPA/WPA2 avec TKIP ou AES (qui sont plus sécurisés).

Couche Sans fil 2 de contrôleur LAN – Matrice de compatibilité de degré de sécurité de la couche 3

Quand vous configurez la Sécurité sur un RÉSEAU LOCAL Sans fil, posez 2 et posez 3 méthodes de Sécurité peut être utilisé dans la conjonction. Cependant, non toutes les méthodes de degré de sécurité de la couche 2 peuvent être utilisées avec toutes les méthodes de degré de sécurité de la couche 3. Cette table affiche la matrice de compatibilité des méthodes pour de la couche 2 et de la couche 3 degré de sécurité prises en charge sur le contrôleur LAN Sans fil.

Mécanisme de sécurité de la couche 2	Mécanisme de sécurité de la couche 3	Compatibilité
Aucune	Aucune	Valide
WPA+WPA2	Aucune	Valide
WPA+WPA2	Authentification Web	Non valide
WPA-PSK/WPA2-PSK	Authentification Web	Valide
WPA+WPA2	Fonction émulation de	Non valide

	Web	
WPA-PSK/WPA2-PSK	Fonction émulation de Web	Valide
WPA+WPA2	Le Web conditionnel réorientent	Valide
WPA+WPA2	Le Web de page de splash réorientent	Valide
WPA+WPA2	Relais VPN	Valide
802.1x	Aucune	Valide
802.1x	**Authentification Web**	Non valide
802.1x	Fonction émulation de Web	Non valide
802.1x	Le Web conditionnel réorientent	Valide
802.1x	Le Web de page de splash réorientent	Valide
802.1x	Relais VPN	Valide
WEP statique	Aucune	Valide
WEP statique	**Authentification Web**	Valide
WEP statique	Fonction émulation de Web	Valide
WEP statique	Le Web conditionnel réorientent	Non valide
WEP statique	Le Web de page de splash réorientent	Non valide
WEP statique	Relais VPN	Valide
802.1x Static-WEP+	Aucune	Valide
802.1x Static-WEP+	**Authentification Web**	Non valide
802.1x Static-WEP+	Fonction émulation de Web	Non valide
802.1x Static-WEP+	Le Web conditionnel réorientent	Non valide
802.1x Static-WEP+	Le Web de page de splash	Non valide

	réorientent	
802.1x Static-WEP+	Relais VPN	Non valide
CKIP	Aucune	Valide
CKIP	Authentification Web	Valide
CKIP	Fonction émulation de Web	Valide
CKIP	Le Web conditionnel réorientent	Non valide
CKIP	Le Web de page de splash réorientent	Non valide
CKIP	Relais VPN	Valide

Informations connexes

- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Support et documentation techniques - Cisco Systems