Matrice de compatibilité de sécurité des couches 2 et 3 du WLC

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Conventions
Solutions Cisco Unified Wireless Network Security
Contrôleur LAN sans fil - Matrice de compatibilité de la sécurité de couche 2 - 3
Informations connexes

Introduction

Ce document fournit la matrice de compatibilité pour les mécanismes de sécurité des couches 2 et 3 pris en charge sur le contrôleur de réseau local sans fil (WLC).

Conditions préalables

Exigences

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)
- Connaissances de base sur les solutions de sécurité sans fil

Composants utilisés

Les informations de ce document sont basées sur un WLC de la gamme Cisco 4400/2100 qui exécute la version 7.0.116.0 du microprogramme

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Solutions Cisco Unified Wireless Network Security

Le réseau sans fil unifié Cisco prend en charge les méthodes de sécurité des couches 2 et 3.

- Sécurité de couche 2
- Sécurité de couche 3 (pour WLAN) ou de couche 3 (pour Guest LAN)

La sécurité de couche 2 n'est pas prise en charge sur les réseaux locaux invités.

Ce tableau répertorie les différentes méthodes de sécurité des couches 2 et 3 prises en charge sur le contrôleur de réseau local sans fil. Ces méthodes de sécurité peuvent être activées à partir de l'onglet **Security** sur la page **WLANs > Edit** du WLAN.

Mécanisme de sécurité de couche 2		
Paramètre		**Description**
Sécurité de couche 2	Aucune	Aucune sécurité de couche 2 sélectionnée.
	WPA+WPA2	Utilisez ce paramètre afin d'activer Wi-Fi Protected Access.
	802.1X	Utilisez ce paramètre afin d'activer l'authentification 802.1x.
	WEP statique	Utilisez ce paramètre afin d'activer le cryptage WEP statique.
	WEP statique + 802.1x	Utilisez ce paramètre afin d'activer les paramètres WEP statique et 802.1x.
	CKIP	Utilisez ce paramètre afin d'activer le protocole CKIP (Cisco Key Integrity Protocol). Fonctionnel sur les modèles AP 1100, 1130 et 1200, mais pas sur 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 les clients par adresse MAC. Configurez localement les clients par adresse MAC dans la page MAC Filters > New. Sinon, configurez les clients sur un serveur RADIUS.	
Mécanisme de sécurité de couche 3 (pour WLAN)		
Paramètre		**Description**
Sécurité de	Aucune	Aucune sécurité de couche 3 sélectionnée.

couche 3	IPsec	Utilisez ce paramètre afin d'activer IPSec. Vous devez vérifier la disponibilité des logiciels et la compatibilité du matériel client avant d'implémenter IPSec. **Remarque :** vous devez disposer du module de sécurité VPN/Enhanced (carte processeur de chiffrement) en option pour activer IPSec. Vérifiez qu'il est installé sur votre contrôleur sur la page Inventaire.
	Passthrough VPN	Utilisez ce paramètre afin d'activer le Passthrough VPN. **Remarque :** cette option n'est pas disponible sur les contrôleurs des gammes Cisco 5500 et Cisco 2100. Cependant, vous pouvez répliquer cette fonctionnalité sur un contrôleur de la gamme Cisco 5500 ou Cisco 2100 en créant un WLAN ouvert à l'aide d'une liste de contrôle d'accès.
Stratégie Web	Cochez cette case pour activer la stratégie Web. Le contrôleur transfère le trafic DNS vers et depuis les clients sans fil avant l'authentification. **Remarque : la** stratégie Web ne peut pas être utilisée en combinaison avec les options IPsec ou VPN Pass-Through. Ces paramètres s'affichent : • Authentication : si vous sélectionnez cette option, l'utilisateur est invité à saisir son nom d'utilisateur et son mot de passe lors de la connexion du client au réseau sans fil. • Passthrough : si vous sélectionnez cette option, l'utilisateur peut accéder directement au réseau sans authentification par nom d'utilisateur et mot de passe. • Redirection Web conditionnelle : si vous sélectionnez cette option, l'utilisateur peut	

	être redirigé de manière conditionnelle vers une page Web particulière une fois l'authentification 802.1X terminée. Vous pouvez spécifier la page de redirection et les conditions sous lesquelles celle-ci se produit sur votre serveur RADIUS. • Redirection Web de la page d'accueil : si vous sélectionnez cette option, l'utilisateur est redirigé vers une page Web particulière une fois l'authentification 802.1X terminée. Une fois la redirection effectuée, l'utilisateur dispose d'un accès complet au réseau. Vous pouvez spécifier la page Web d'accueil sur votre serveur RADIUS. • En cas d'échec du filtre MAC : active les échecs du filtre MAC d'authentification Web.
ACL de pré-authentification	Sélectionnez la liste de contrôle d'accès à utiliser pour le trafic entre le client et le contrôleur.
Remplacer la configuration globale	S'affiche si vous sélectionnez Authentication. Cochez cette case afin de remplacer le jeu de configuration d'authentification globale sur la page de connexion Web.
Type d'authentification Web	S'affiche si vous sélectionnez Stratégie Web et Remplacer la configuration globale. Sélectionnez un type d'authentification Web : • Interne • Personnalisé (téléchargé) Login Page : sélectionnez une page de connexion dans la liste déroulante.Page Échec de connexion : sélectionnez une page de connexion qui s'affiche pour le client si l'authentification Web échoue.Page Déconnexion : sélectionnez une page de connexion qui s'affiche pour le client lorsque l'utilisateur se déconnecte du système. • Externe (redirection vers un serveur externe) URL : saisissez l'URL du serveur externe.
Saisie e-mail	S'affiche si vous sélectionnez Passthrough. Si vous sélectionnez cette option, vous êtes invité à saisir votre adresse e-mail lors de la connexion au réseau.

Mécanisme de sécurité de couche 3 (pour le réseau local invité)		
Paramètre		**Description**
Sécurité de couche 3	Aucune	Aucune sécurité de couche 3 sélectionnée.
	Authentification Web	Si vous sélectionnez cette option, vous êtes invité à saisir un nom d'utilisateur et un mot de passe lors de la connexion du client au réseau.
	Passthrough Web	Si vous sélectionnez cette option, vous pouvez accéder directement au réseau sans authentification par nom d'utilisateur et mot de passe.
ACL de pré-authentification		Sélectionnez la liste de contrôle d'accès à utiliser pour le trafic entre le client et le contrôleur.
Remplacer la configuration globale		Cochez cette case afin de remplacer le jeu de configuration d'authentification globale sur la page de connexion Web.
Type d'authentification Web		S'affiche si vous sélectionnez Remplacer la configuration globale. Sélectionnez un type d'authentification Web : • Interne • Personnalisé (téléchargé) Login Page : sélectionnez une page de connexion dans la liste déroulante.Page Échec de connexion : sélectionnez une page de connexion qui s'affiche pour le client si l'authentification Web échoue.Page Déconnexion : sélectionnez une page de connexion qui

	s'affiche pour le client lorsque l'utilisateur se déconnecte du système. • Externe (redirection vers un serveur externe) URL : saisissez l'URL du serveur externe.
Saisie e-mail	S'affiche si vous sélectionnez Passthrough Web. Si vous sélectionnez cette option, vous êtes invité à saisir votre adresse e-mail lors de la connexion au réseau.

Remarque : dans le logiciel du contrôleur version 4.1.185.0 ou ultérieure, CKIP est pris en charge pour une utilisation uniquement avec le WEP statique. Il n'est pas pris en charge avec le WEP dynamique. Par conséquent, un client sans fil configuré pour utiliser CKIP avec WEP dynamique ne peut pas s'associer à un réseau local sans fil configuré pour CKIP. Cisco recommande d'utiliser soit le WEP dynamique sans CKIP (qui est moins sécurisé), soit le WPA/WPA2 avec TKIP ou AES (qui sont plus sécurisés).

Contrôleur LAN sans fil - Matrice de compatibilité de la sécurité de couche 2 - 3

Lorsque vous configurez la sécurité sur un réseau local sans fil, les méthodes de sécurité de couche 2 et de couche 3 peuvent être utilisées conjointement. Cependant, toutes les méthodes de sécurité de couche 2 ne peuvent pas être utilisées avec toutes les méthodes de sécurité de couche 3. Ce tableau présente la matrice de compatibilité des méthodes de sécurité des couches 2 et 3 prises en charge sur le contrôleur de réseau local sans fil.

Mécanisme de sécurité de couche 2	Mécanisme de sécurité de 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	Passthrough Web	Non valide
WPA-PSK/WPA2-PSK	Passthrough Web	Valide
WPA+WPA2	Redirection Web conditionnelle	Valide
WPA+WPA2	Redirection Web	Valide

	de la page de démarrage	
WPA+WPA2	VPN-PassThrough	Valide
802.1x	Aucune	Valide
802.1x	Authentification Web	Non valide
802.1x	Passthrough Web	Non valide
802.1x	Redirection Web conditionnelle	Valide
802.1x	Redirection Web de la page de démarrage	Valide
802.1x	VPN-PassThrough	Valide
WEP statique	Aucune	Valide
WEP statique	Authentification Web	Valide
WEP statique	Passthrough Web	Valide
WEP statique	Redirection Web conditionnelle	Non valide
WEP statique	Redirection Web de la page de démarrage	Non valide
WEP statique	VPN-PassThrough	Valide
Statique-WEP+ 802.1x	Aucune	Valide
Statique-WEP+ 802.1x	Authentification Web	Non valide
Statique-WEP+ 802.1x	Passthrough Web	Non valide
Statique-WEP+ 802.1x	Redirection Web conditionnelle	Non valide
Statique-WEP+ 802.1x	Redirection Web de la page de démarrage	Non valide
Statique-WEP+ 802.1x	VPN-PassThrough	Non valide
CKIP	Aucune	Valide
CKIP	Authentification Web	Valide
CKIP	Passthrough Web	Valide
CKIP	Redirection Web conditionnelle	Non valide
CKIP	Redirection Web de la page de démarrage	Non valide
CKIP	VPN-PassThrough	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 du contrôleur LAN sans fil Cisco, version 7.0.116.0
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.