Exclusion du client 802.1X sur un WLC AireOS

Contenu

Introduction

Ce document décrit l'exclusion du client 802.1X sur un contrôleur LAN sans fil AireOS (WLC). L'exclusion du client 802.1X est une option importante à utiliser sur un authentificateur 802.1X tel qu'un WLC. Ceci afin d'empêcher une surcharge de l'infrastructure du serveur d'authentification par les clients EAP (Extensible Authentication Protocol) qui sont hyperactifs ou fonctionnent de manière incorrecte.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WLC Cisco AireOS
- Protocole 802.1X
- RADIUS (Remote Authentication Dial-In User Service)
- Identity Service Engine (ISE)

Components Used

Les informations de ce document sont basées sur AireOS.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Dossiers utilisateur

Exemples de cas d'utilisateur :

- Un demandeur EAP configuré avec des informations d'identification incorrectes. La plupart des demandeurs, tels que les demandeurs EAP, cessent les tentatives d'authentification après quelques échecs successifs. Cependant, certains demandeurs du PAE continuent de tenter de se réauthentifier en cas d'échec, peut-être plusieurs fois par seconde. Certains clients surchargent les serveurs RADIUS et provoquent un déni de service (DoS) pour l'ensemble du réseau.
- Après un basculement majeur du réseau, des centaines ou des milliers de clients EAP peuvent tenter simultanément de s'authentifier. En conséquence, les serveurs d'authentification peuvent être surchargés et fournir une réponse lente. Si le délai d'attente des clients ou de l'authentificateur est dépassé avant le traitement de la réponse lente, un cercle vicieux peut se produire lorsque les tentatives d'authentification continuent à expirer, puis essayez de traiter à nouveau la réponse.

  Note: Un mécanisme de contrôle d'admission est nécessaire pour permettre aux tentatives d'authentification de réussir.

Fonctionnement de l'exclusion de client 802.1X

L'exclusion de client 802.1X empêche les clients d'envoyer des tentatives d'authentification pendant une période après des échecs d'authentification 802.1X excessifs. Sur un WLC AireOS 802.1X, l'exclusion de client est activée globalement sous **Security > Wireless Protection Policies > Client Exclusion Policies** par défaut et peut être vue dans cette image.

L'exclusion de client peut être activée ou désactivée par WLAN. Par défaut, il est activé avec un délai d'attente de 60 secondes avant AireOS 8.5 et de 180 secondes à partir d'AireOS 8.5.

Paramètres d'exclusion pour protéger les serveurs RADIUS de la surcharge

Afin de valider que le serveur RADIUS est protégé contre la surcharge due à des clients sans fil qui fonctionnent incorrectement, vérifiez que ces paramètres sont en vigueur :

- **Les échecs excessifs d'authentification 802.1X** sont sélectionnés dans les stratégies globales d'exclusion de client du WLC.
- **L'exclusion du client** est activée dans les paramètres avancés du WLAN.
- **La valeur du délai d'attente d'exclusion du client** est définie sur 60 à 300 secondes.
  Note: Des valeurs supérieures à 300 secondes offrent une meilleure protection mais peuvent déclencher des plaintes de la part des utilisateurs.
- Configurer les compteurs EAP AireOS et les paramètres PEAP (Protected Extensible Authentication Protocol) ISE

Problèmes empêchant l'exclusion 802.1X de fonctionner

Plusieurs paramètres de configuration, dans le WLC et dans le serveur RADIUS, peuvent empêcher l'exclusion de client 802.1X de fonctionner.

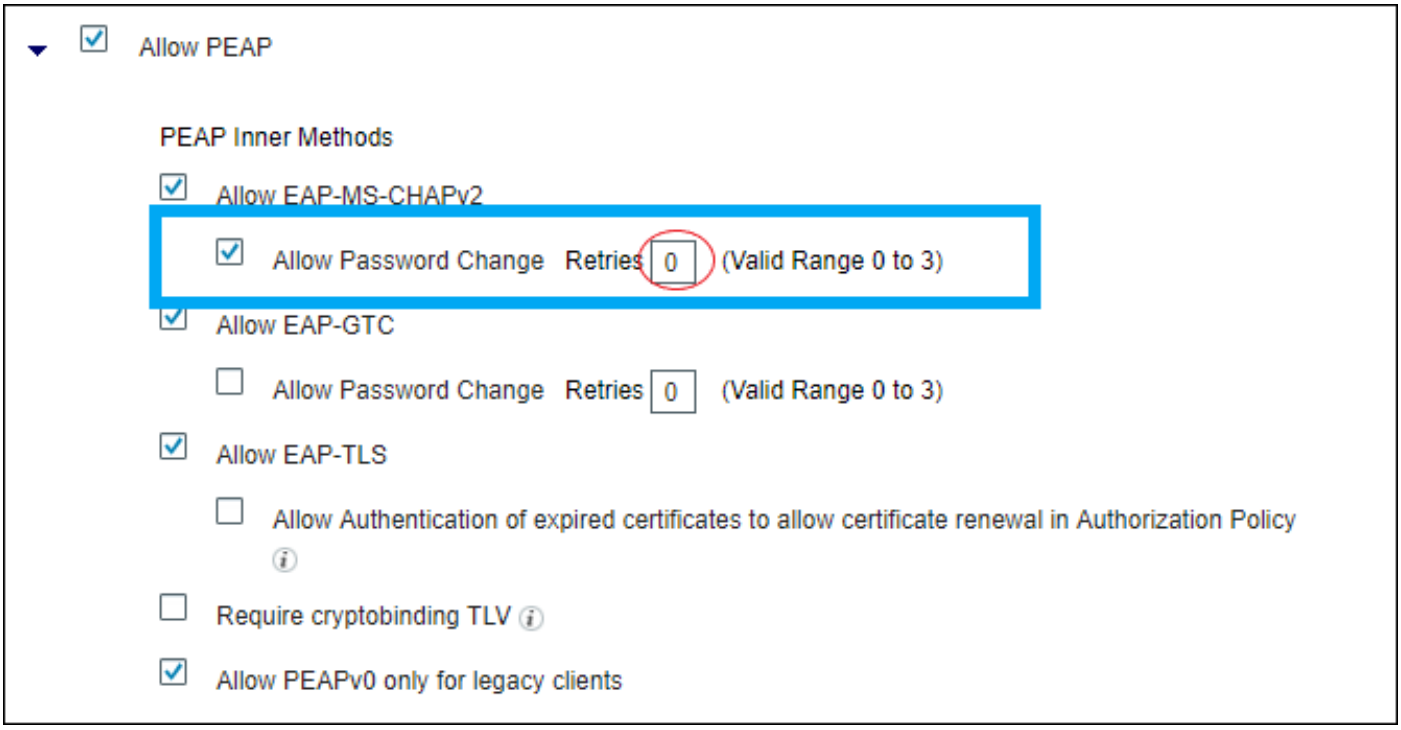
Clients non exclus en raison des paramètres du temporisateur EAP du WLC

Par défaut, les clients sans fil ne sont pas exclus lorsque **Client Exclusion** est défini sur Activé sur le WLAN. Ceci est dû à de longs délais d'expiration EAP par défaut de 30 secondes qui font qu'un client qui se comporte mal ne doit jamais atteindre suffisamment d'échecs successifs pour déclencher une exclusion. Configurez des délais d'attente EAP plus courts avec un nombre accru de retransmissions pour permettre l'application de l'exclusion du client 802.1X. Voir l'exemple de délai d'attente.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

Clients non exclus en raison des paramètres PEAP ISE

Pour que l'exclusion du client 802.1X fonctionne, le serveur RADIUS doit envoyer un Access-Reject en cas d'échec de l'authentification. Si le serveur RADIUS est ISE et si le PEAP est utilisé, l'exclusion peut ne pas se produire et dépend des paramètres du PEAP ISE. Dans ISE, accédez à **Policy > Results** > **Authentication** > **Allowed Protocols** > **Default Network Access** comme indiqué dans l'image.



Si vous définissez **Retries** (cerclé en rouge sur la droite) sur 0, ISE devrait envoyer Access-Reject immédiatement au WLC, qui devrait activer le WLC afin d'exclure le client (s'il essaie trois fois d'authentifier).

> **Remarque :** Le paramètre **Retries** est quelque peu indépendant de la case **Autoriser la modification du mot de passe**, c'est-à-dire que la valeur **Retries** sera honorée, même si **Autoriser la modification du mot de passe** n'est pas cochée. Cependant, si **Retries** est défini sur 0, **Allow Password Change** ne fonctionnera pas.

Informations connexes

- ID de bogue Cisco : CSCsq16858
- Empêcher les pales de fusion de réseau RADIUS sans fil à grande échelle
- Support et documentation techniques - Cisco Systems