exclusion de client de 802.1X sur un AireOS WLC

TAC

ID de document : 117714

Mis à jour : Juin 03, 2014

Contribué par Aaron Léonard et Shankar Ramanathan, ingénieurs TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Réseau local sans fil (WLAN)

Contenu

Introduction
Cas d'utilisation
Clients WLC non exclus quand l'exclusion de 802.1X est activée
Informations connexes
Cisco relatif prennent en charge des discussions de la Communauté

Introduction

Ce document décrit le client Exlusion de 802.1X sur un contrôleur LAN Sans fil d'AireOS (WLC). l'exclusion de client de 802.1X est une importante option d'avoir sur un authentificateur 1X comme un WLC. C'est afin d'empêcher une surcharge de l'infrastructure de serveur d'authentification par les clients de Protocole EAP (Extensible Authentication Protocol) qui sont hyperactifs ou fonction incorrectement.

Cas d'utilisation

Les cas d'utilisation d'exemple incluent :

- Un suppliant d'EAP peut être configuré avec les qualifications incorrectes. La plupart des suppliants, tels que des suppliants d'EAP, cessent des tentatives d'authentification après quelques pannes successives. Cependant, quelques suppliants d'EAP continuent des

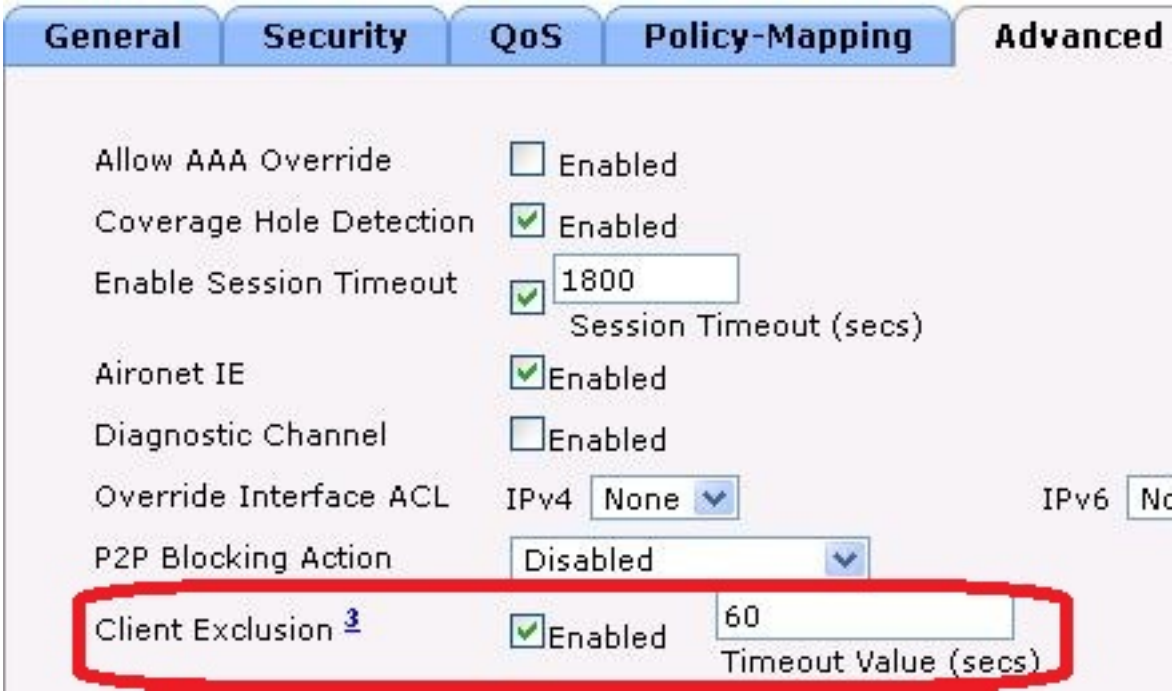
tentatives d'authentifier à nouveau lors de la panne, probablement beaucoup de fois par seconde. Quelques clients surchargent des serveurs de RAYON et entraînent un Déni de service (DOS) pour le réseau entier.

- Après un Basculement de réseau important, les centaines ou les milliers de clients d'EAP pourraient simultanément tenter d'authentifier. En conséquence, les serveurs d'authentification pourraient être surchargés et fournir une réponse lente. Si le temps de clients ou d'authentificateur avant que la réponse lente soit traitée, alors un cercle vicieux peuvent se produire où les tentatives d'authentification continuent, et puis à chronométrer essayent de traiter la réponse de nouveau.

  Remarque: Un mécanisme de contrôle d'admission est exigé afin de permettre des tentatives d'authentification de réussir.

l'exclusion de 802.1X empêche les clients qui déclenchent la surcharge pendant 30 secondes à plusieurs minutes après panne, qui permet à des authentifications normales pour réussir. Un AireOS WLC a nominalement l'exclusion de client de 802.1X globablly activée dans le cadre des stratégies de Sécurité > de protection sans fil par défaut. Voyez les stratégies affichées ici.

L'exclusion de client pourrait être activée ou désactivée sur une base par-WLAN. Par défaut il est activé avec un délai d'attente de 60 secondes.



Cependant, dû pour transférer des configurations de délai d'attente et de retransmission d'EAP, l'exclusion de 802.1X ne la prend jamais effet.

Clients WLC non exclus quand l'exclusion de 802.1X est activée

Des clients WLC ne sont pas exclus quand l'exclusion de 802.1X est activée sur le WLAN. C'est dû à de longs délais d'attente par défaut d'EAP de 30 secondes qui entraînent un client qui se conduit mal pour ne jamais frapper assez de manques successifs de déclencher une exclusion. Configurez des délais d'attente plus courts d'EAP avec des nombres accrus de retransmissions pour permettre à l'exclusion de 802.1X pour le prendre effet. Voyez l'exemple de délai d'attente ici.

```
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
```

Assurez-vous que le serveur de RAYON est protégé contre la surcharge due aux clients sans fil qui fonctionnent inexactement et vérifie que ces configurations sont en vigueur :

- « Des échecs d'authentification excessifs de 802.1X » est sélectionnés dans les stratégies globales d'exclusion du client du WLC.
- L'exclusion de client est activée dans les paramètres avancés du WLAN.
- Le délai d'attente d'exclusion de client est placé à 60 à 300 secondes.

  Remarque: Le supérieur à de valeurs 300 secondes assurent une meilleure protection mais pourraient déclencher des plaintes d'utilisateur.

  Avertissement : Quelques suppliants ont besoin de plus longs délais d'attente que d'autres. Par exemple, si des mots de passe une fois sont utilisés, le délai d'inactivité de demande d'identité d'EAP pourrait avoir besoin de 45 secondes afin de permettre à l'utilisateur pour écrire un nouveau PIN. De l'authentification Protocol-flexible extensible lente d'Authetication par l'intermédiaire des suppliants de protocole sécurisé (EAP-FAST) pourrait exiger d'un délai d'attente plus court de 20 secondes afin de faciliter le ravitaillement protégé du contrôle

d'accès (PAC).

Informations connexes

- ID de bogue Cisco CSCsq16858
- Support et documentation techniques - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Mis à jour : Juin 03, 2014
ID de document : 117714