Configurez l'écoulement d'invité avec ISE 2.0 et Aruba WLC

Contenu

Introduction

Les descrbies de ce document fait un pas pour configurer des portails d'invité avec le contrôleur LAN Sans fil d'Aruba (WLC). Du soutien de version 2.0 du Cisco Identity Services Engine (ISE) de l'accès de réseau de tiers les périphériques (NAD) est introduits. ISE prend en charge actuellement l'intégration avec la radio d'Aruba pour l'invité, posture et Bring Your Own Device (BYOD) circule.

> Remarque: Cisco n'est pas responsable de la configuration ou du soutien des périphériques d'autres constructeurs.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

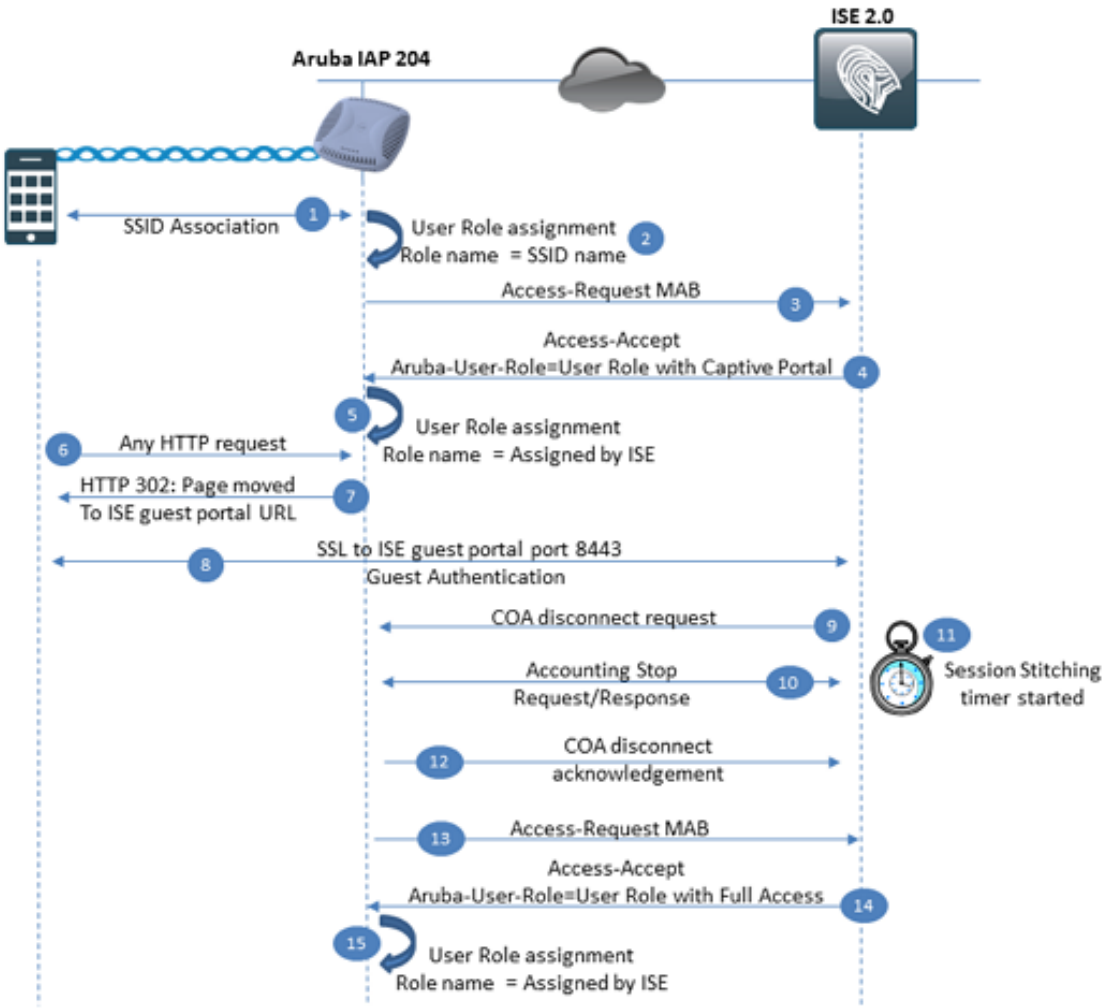
- Configuration d'Aruba ILI
- Écoulement d'invité sur ISE

Composants utilisés

- Logiciel 6.4.2.3 d'Aruba ILI 204
- Logiciel Cisco Identity Services Engine 2.0

Informations générales

Écoulement d'invité



Étape 1. L'utilisateur est associé à l'ensemble de services Identifer (SSID). Le SSID peut être configuré comme ouvert ou avec l'authentification principale pré-partagée.

Étape 2. Aruba s'applique le rôle de l'utilisateur à cette connexion. Le premier rôle de l'utilisateur est toujours SSID lui-même. Le rôle de l'utilisateur contient différentes configurations comme le VLAN, la restriction de contrôle d'accès, la configuration Captif-portaile et plus. Dans le rôle de l'utilisateur en cours de par défaut d'exemple assigné au SSID a seulement Autorisation-toute déclaration.

Étape 3. Le SSID est configuré pour fournir le filtrage MAC au-dessus du serveur RADIUS externe. L'Access-demande de MAB de rayon (dérivation d'authentification MAC) est envoyée à

ISE.

Étape 4. Au temps d'évaluation de stratégie ISE sélectionne le profil d'autorisation pour l'invité. Ce profil d'autorisation contient le type d'Access égal à ACCESS_ACCEPT et l'Aruba-Utilisateur-rôle égal au rôle de l'utilisateur de nom configuré localement sur Aruba WLC (contrôleur LAN Sans fil). Ce rôle de l'utilisateur est configuré pour Captif-portail et le trafic est réorienté vers ISE.

Rôles de l'utilisateur d'Aruba

Le composant principal qui est utilisé par Aruba WLC est rôle de l'utilisateur. Le rôle de l'utilisateur définit la restriction d'accès applicable à l'utilisateur au moment de la connexion. La restriction d'Access peut inclure : Redirection, liste de contrôle d'accès, VLAN (réseau local virtuel), limite de bande passante et autres portaiux captifs. Chaque SSID qui existe sur Aruba WLC a le rôle de l'utilisateur par défaut où le rôle de l'utilisateur est égal au nom SSID, tous les utilisateurs connectés à la particularité SSID obtiennent au commencement des restrictions de rôle par défaut. Le rôle de l'utilisateur peut être remplacé par le serveur de rayon, dans ce cas Access-Recevoir devrait contenir l'Aruba-Utilisateur-rôle spécifique d'attribut de constructeur d'Aruba. La valeur de cet attribut est utilisée par WLC pour trouver le rôle de l'utilisateur local.

Étape 5. Avec des contrôles du l'Aruba-Utilisateur-rôle WLC d'attribut localement pour des rôles de l'utilisateur configurés et applique requis.

Étape 6. L'utilisateur initie la demande de HTTP dans le navigateur.

Étape 7. Demande d'interceptions d'Aruba WLC en raison du rôle de l'utilisateur configuré pour le portail captif. Comme une réponse à cette demande WLC renvoie la page du code 302 de HTTP déplacée avec le portail d'invité ISE comme nouveau emplacement.

Étape 8. L'utilisateur établit la connexion SSL à ISE sur le port 8443, et fournit le nom d'utilisateur/mot de passe dans le portail d'invité.

Étape 9. ISE envoie le message de demande de débranchement COA à Aruba WLC.

Étape 10. Après que le message WLC de débranchement COA relâche la connexion avec l'utilisateur et informe ISE que la connexion devrait être terminée utilisant le message de Comptabilité-demande de rayon (arrêt). ISE doit confirmer que ce message a été reçu avec la comptabilité.

Étape 11. ISE met en marche le temporisateur piquant de session. Ce temporisateur est utilisé pour lier la session avant et après le COA ensemble. Pendant ce temps ISE se souvient tous les paramètres de session comme le nom d'utilisateur, etc. La deuxième tentative d'authentification doit être faite avant que ce temporisateur expirent pour sélectionner la stratégie correcte d'autorisation pour le client. Au cas où si le temporisateur expire, la nouvelle Access-demande sera interprétée comme session complètement nouvelle et stratégie d'autorisation avec l'invité Redirect sera appliquée de nouveau.

Étape 12. Aruba WLC confirme la demande de débranchement précédemment reçue COA avec l'accusé de réception de débranchement COA.

Étape 13. Aruba WLC envoie la nouvelle Access-demande de rayon de MAB.

Étape 14. Au temps d'évaluation de stratégie ISE sélectionne le profil d'autorisation pour l'invité après authentification. Ce profil d'autorisation contient le type d'Access égal à ACCESS_ACCEPT

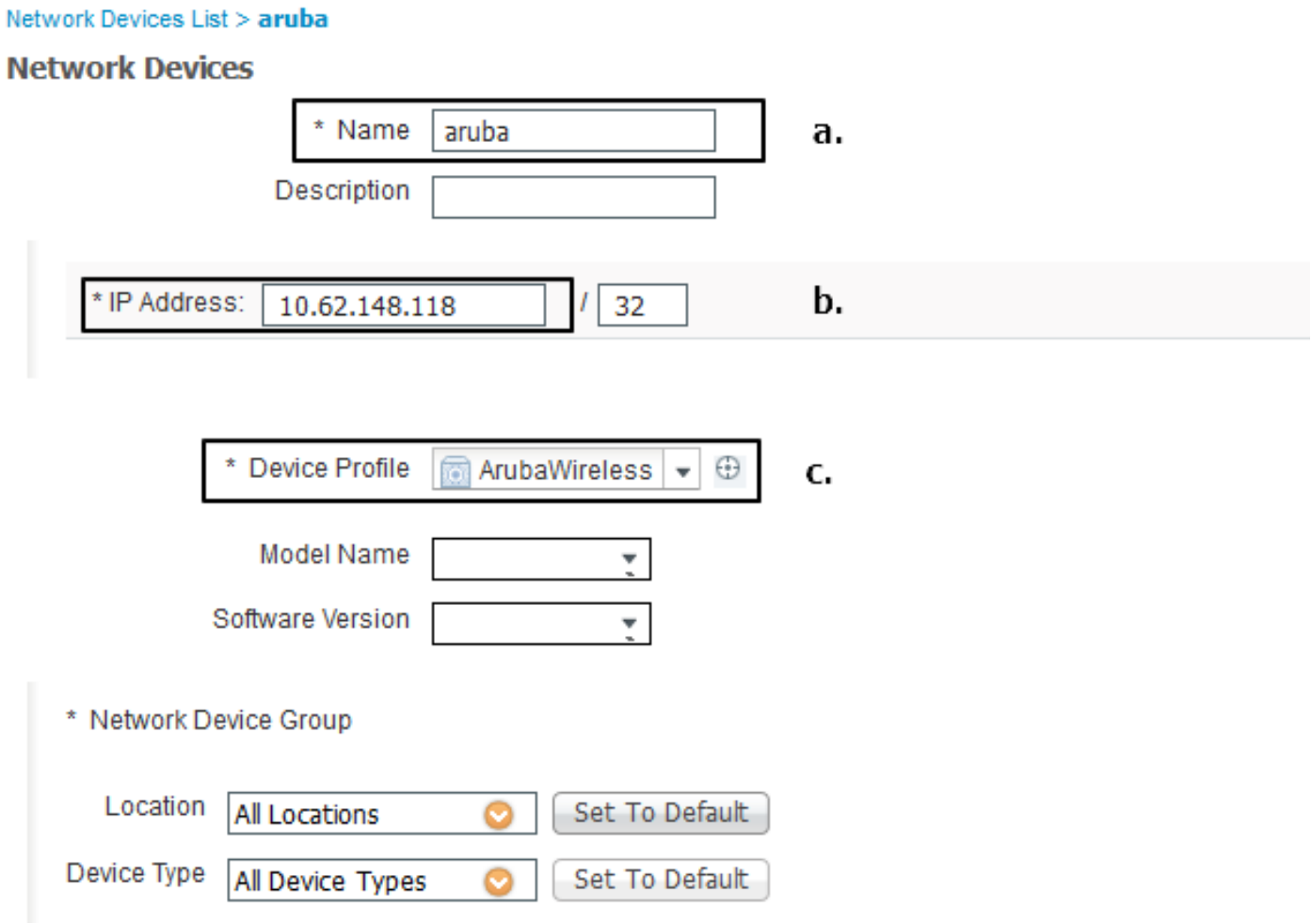
et l'Aruba-Utilisateur-rôle égal au rôle de l'utilisateur de nom configuré localement sur Aruba WLC. Ce rôle de l'utilisateur configuré pour permettre à tous le trafic.

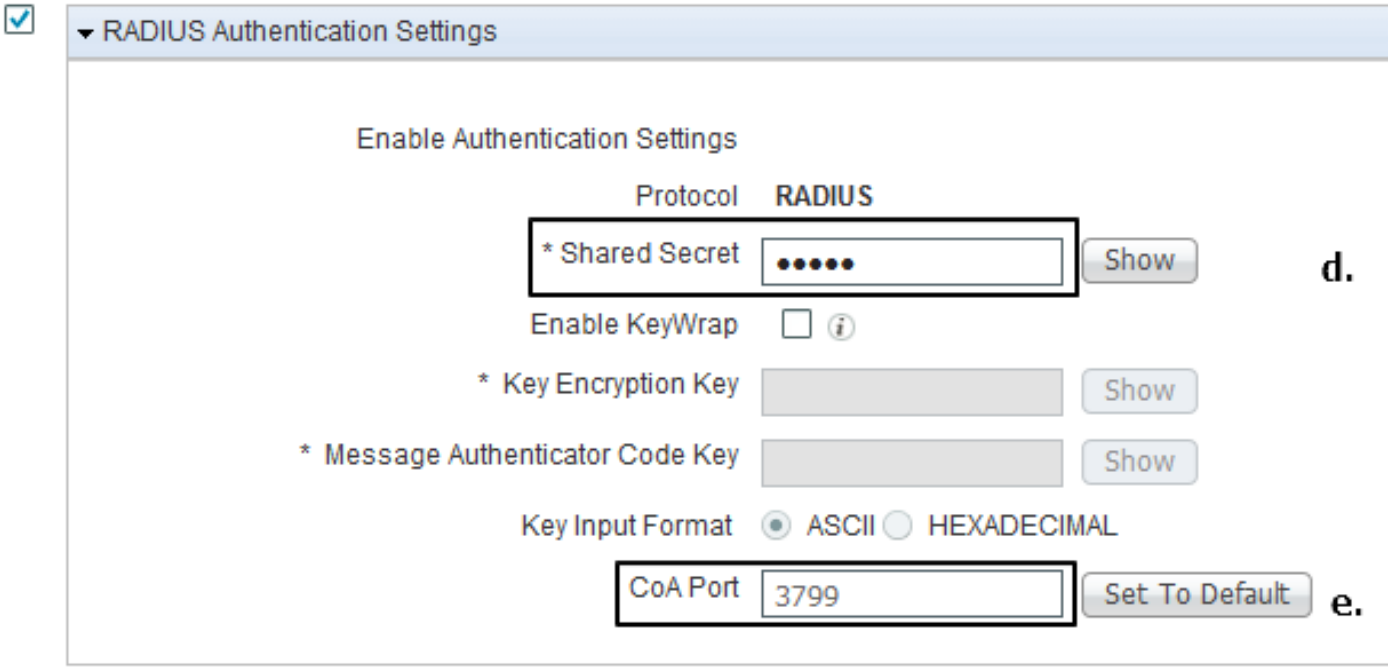
Étape 15. Avec l'Aruba-Utilisateur-rôle d'attribut WLC vérifie des rôles de l'utilisateur localement configurés et applique exigé.

Configurez

Étape 1. Ajoutez Aruba WLC comme NAD dans ISE.

Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau** et cliquez sur Add

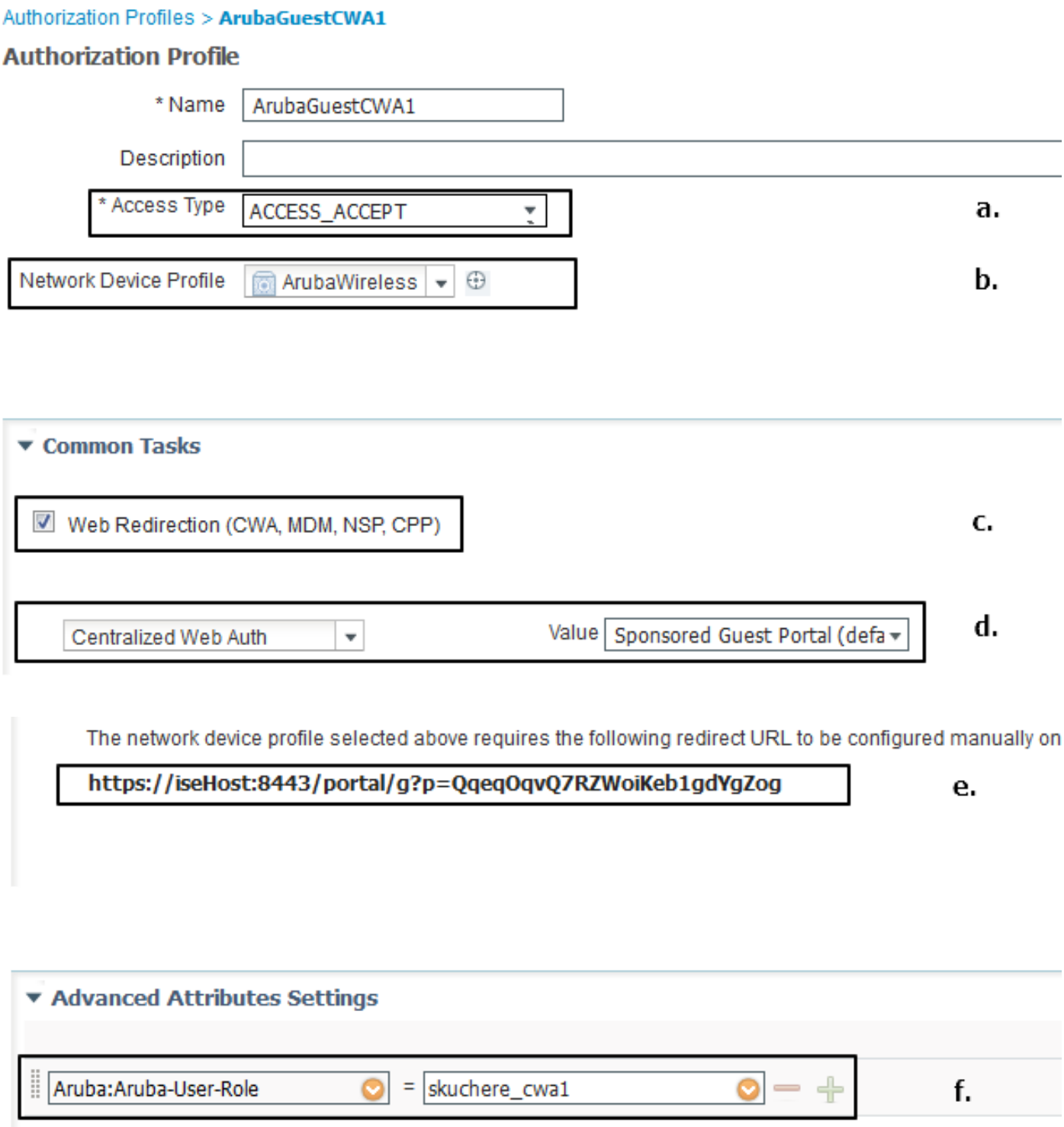




1. Fournissez le nom du périphérique d'accès au réseau (NAD).
2. Spécifiez l'adresse IP NAD.
3. Choisissez le profil de périphérique de réseau. Pour Aruba WLC vous pouvez utiliser le profil intégré ArubaWireless.
4. Fournissez la clé pré-partagée.
5. Définissez le port COA, le port UDP en cours 3799 d'utilisation d'exemple de forme de périphérique pour le COA.

Étape 2. Configurez les profils d'autorisation.

Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > le profil d'autorisation** et cliquez sur Add. D'abord vous devez créer le profil d'autorisation pour l'authentification Web centrale (CWA) réorientez, suivant les indications de l'image.

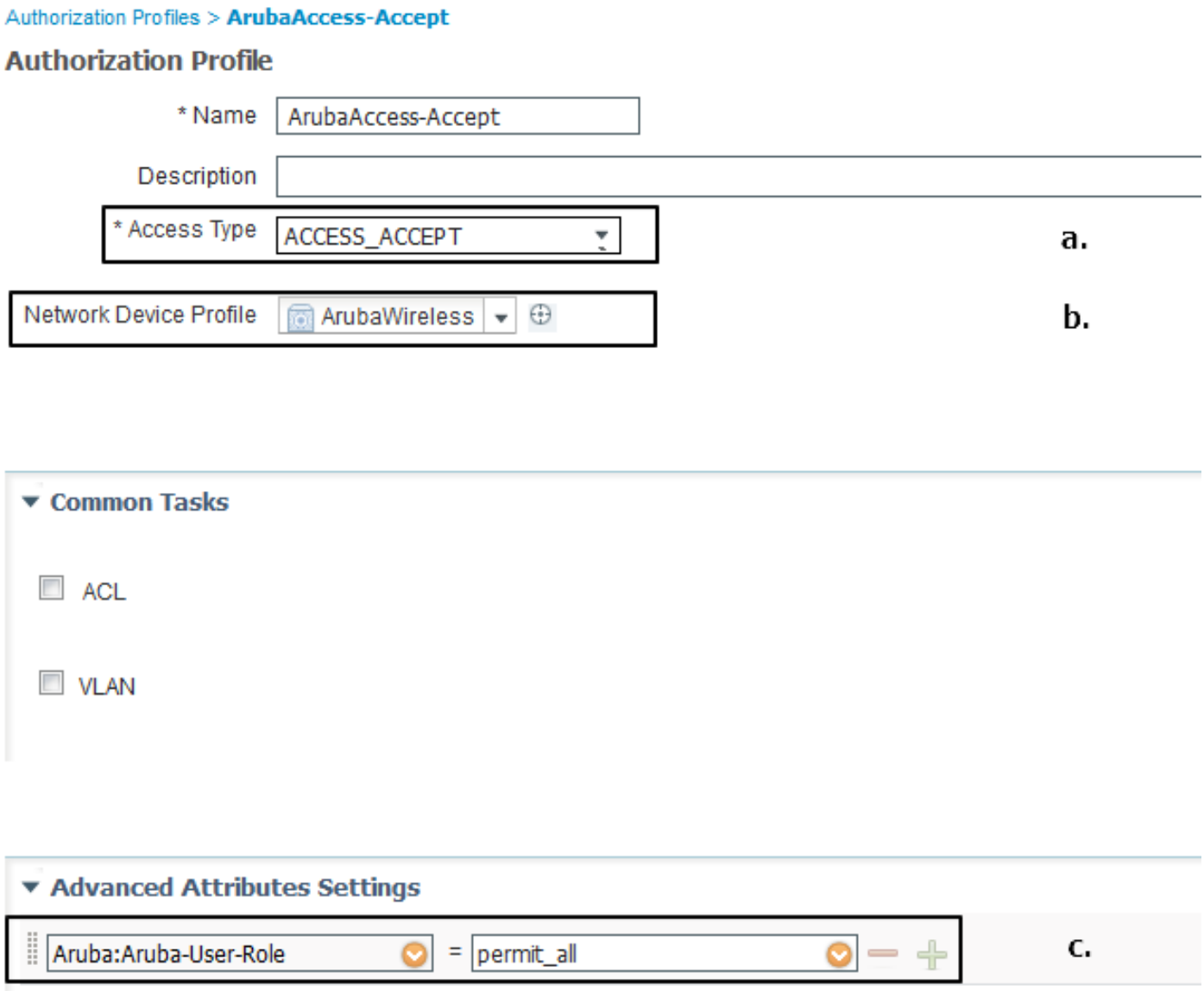


Remarque: Par défaut tous les profils d'autorisation ont le type de périphérique de réseau égal à Cisco. Si NAD lui-même est configuré comme ArubaWireless et profil d'autorisation est créée pour l'autre type de périphérique, ce profil n'est jamais apparié pour ce périphérique.

1. Définissez l'Access-**type** comme Access-**reçoivent**.
2. Dans le **profil de périphérique ArubaWireless** choisi de réseau.
3. Chargez en commun la section, option de **redirection de Web d'**enable.
4. Comme portail **authentique** et choisi d'un **Web centralisé** choisi de type de redirection d'invité que vous voudriez utiliser pour la redirection.
5. L'URL qu'ISE présente devrait être défini sur Aruba WLC en tant qu'URL captif externe de portail.

6. Dans l'**attribut avancé les configurations** sectionnent, définissent le rôle de l'utilisateur de valeur d'attribut d'Aruba.

Le deuxième profil d'autorisation devrait être créé pour fournir l'accès pour des utilisateurs d'invité après l'authentification portaile :



1. Définissez l'Access-**type** comme Access-**reçoivent**.
2. Dans le **profil de périphérique ArubaWireless** choisi de **réseau**.
3. Dans la section **avancée de configurations d'attribut** définissez le rôle de l'utilisateur de valeur d'attribut d'Aruba. Plus tard vous configurerez le rôle de l'utilisateur local sur Aruba WLC avec le même nom.

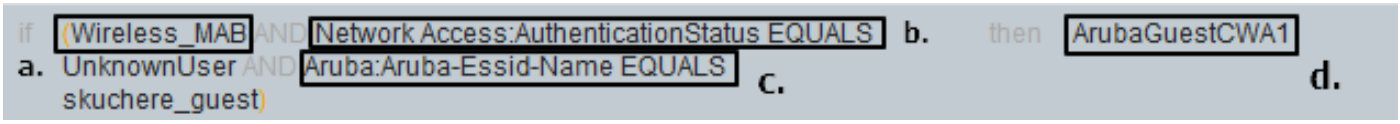
Étape 3. Configurez la stratégie d'autorisation.

La première stratégie d'autorisation est responsable de la redirection d'utilisateur au portail d'invité. Dans le cas le plus simple, vous pouvez utiliser construit en état composé

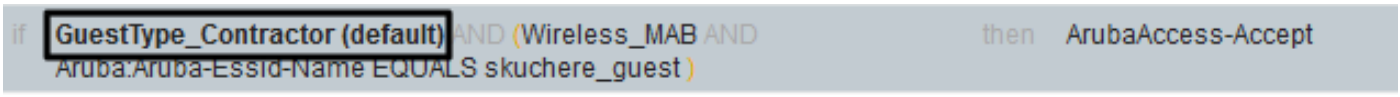
- Wireless_MAB (A.) et
- Égal d'AuthenticationStatus d'accès au réseau à l'utilisateur inconnu (B.) et
- Aruba-Essid-nom d'Aruba égal à votre nom de l'invité SSID (C.).

Pour cette stratégie, configurez le profil d'autorisation avec le portail d'invité de redirect to en

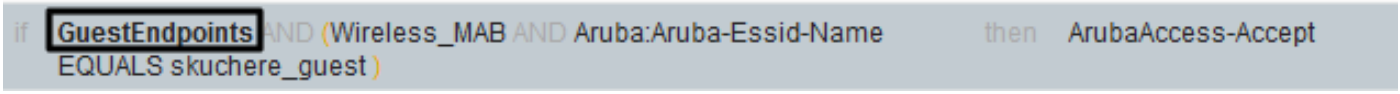
conséquence (le D.)



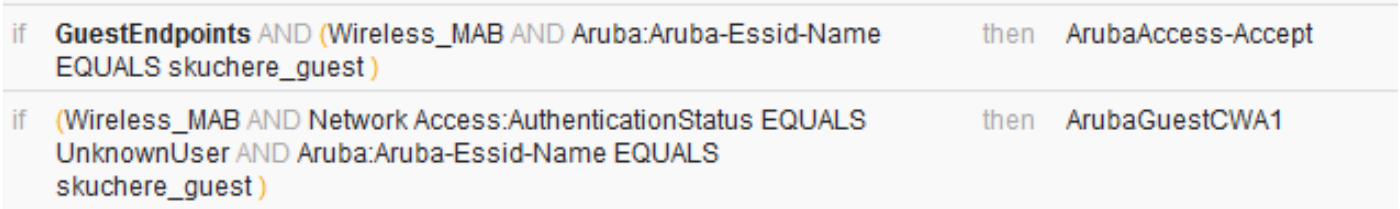
La deuxième stratégie d'autorisation devrait fournir l'accès pour l'utilisateur d'invité après authentification par l'intermédiaire du portail. Cette stratégie peut se fonder sur des données de session (écoulement d'invité de groupe d'identité de l'utilisateur/cas d'utilisation et ainsi de suite). Dans ce scénario l'utilisateur devrait rebrancher avant que le temporisateur piquant de session expirent :



Pour se protéger contre l'expiration de temporisation piquante de session vous pouvez compter sur des données de point final au lieu des données de session. Par défaut, le portail commandité d'invité sur ISE 2.0 est configuré pour l'enregistrement automatique de périphérique d'invité (le périphérique d'invité est automatiquement placé dans le groupe d'identité de point final de Guest_Endpoints). Ce groupe peut être utilisé comme condition :

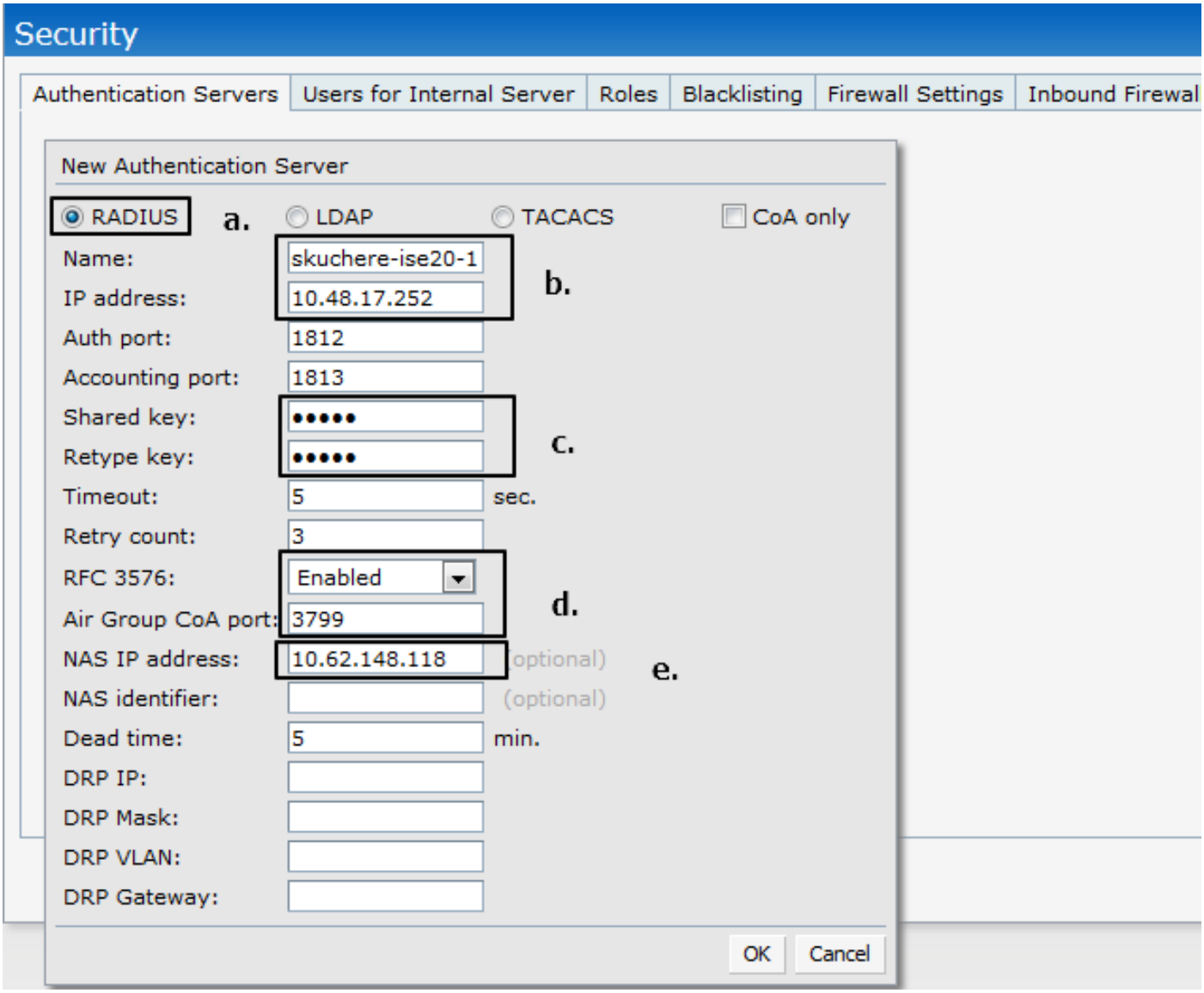


Stratégie d'autorisation dans l'ordre approprié :



Étape 4. Configurez le serveur de rayon sur Aruba.

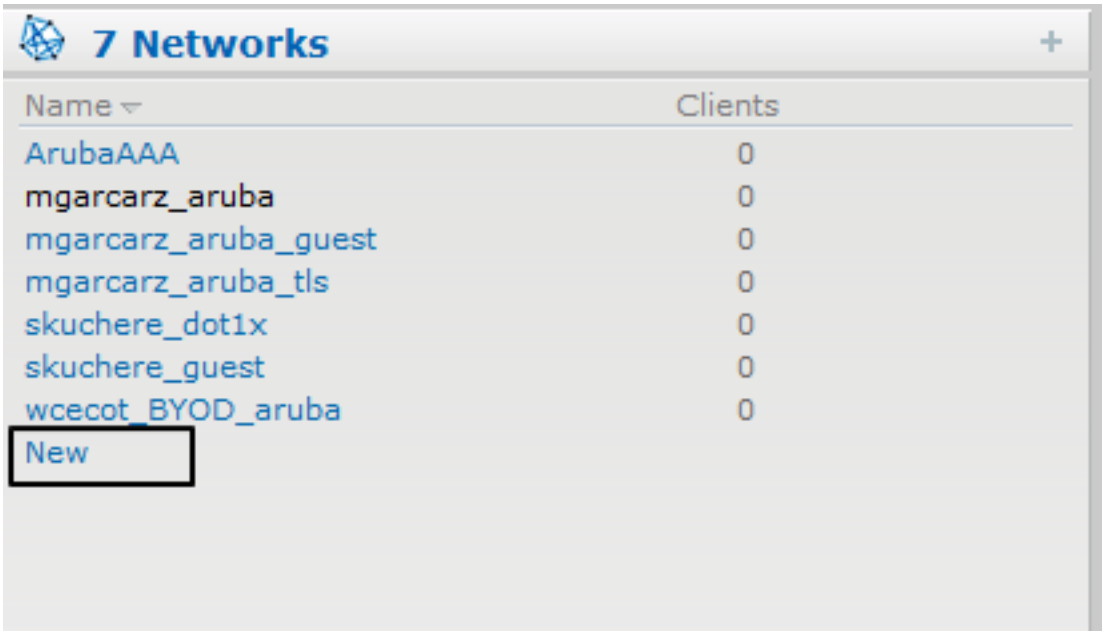
Naviguez vers des **serveurs de Sécurité > d'authentification** et cliquez sur New **:**



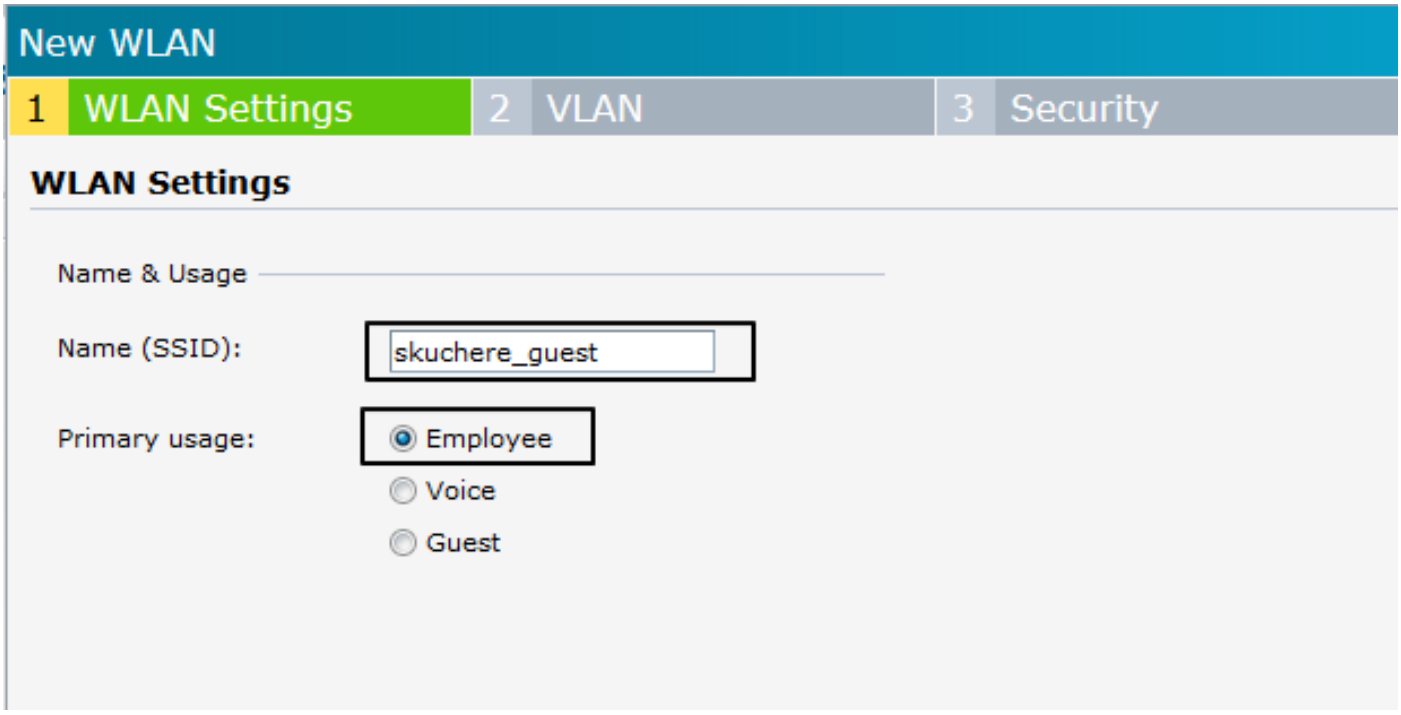
1. Choisissez le RAYON comme protocole AAA.
2. Définissez le nom du serveur et l'adresse IP d'AAA.
3. Spécifiez la clé pré-partagée.
4. Activez le support RFC 3576 et définissez le port COA.
5. Spécifiez l'IP d'interface de gestion d'Aruba WLC comme adresse IP de NAS.

Étape 5. Créez l'invité SSID sur Aruba.

Dans le **nouveau** choisi de page de tableau de bord à la fin de la liste des réseaux. L'assistant de création SSID devrait commencer. Suivez les étapes d'assistant.

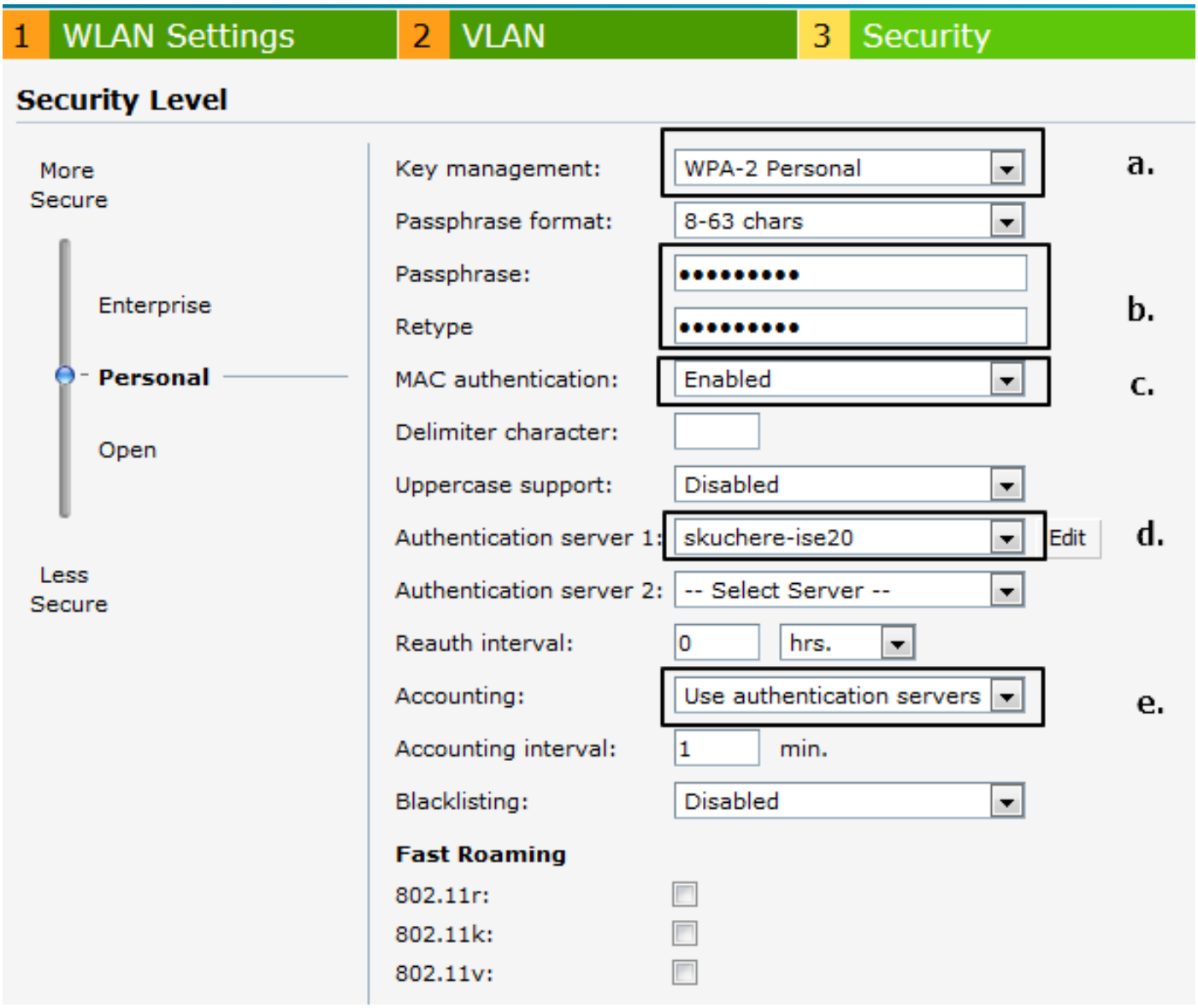


Étape 1. Définissez le nom SSID et le type choisi SSID. Ici, l'employé de type SSID est utilisé. Ce type SSID n'a le rôle par défaut avec l'autorisation tous et aucune application portaile captive. En outre, vous pouvez choisir l'invité de type. Dans un tel scénario vous devriez définir les configurations portailes captives pendant la configuration SSID.



Étape 2. VLAN et affectation d'adresse IP. Ici, des configurations sont laissées comme par défaut, suivant les indications de l'image.

Étape 3. Paramètres de sécurité. Pour l'invité SSID vous pouvez sélectionner vous ouvrez ou personnel. Personnel exige la clé de pré-lambeau.



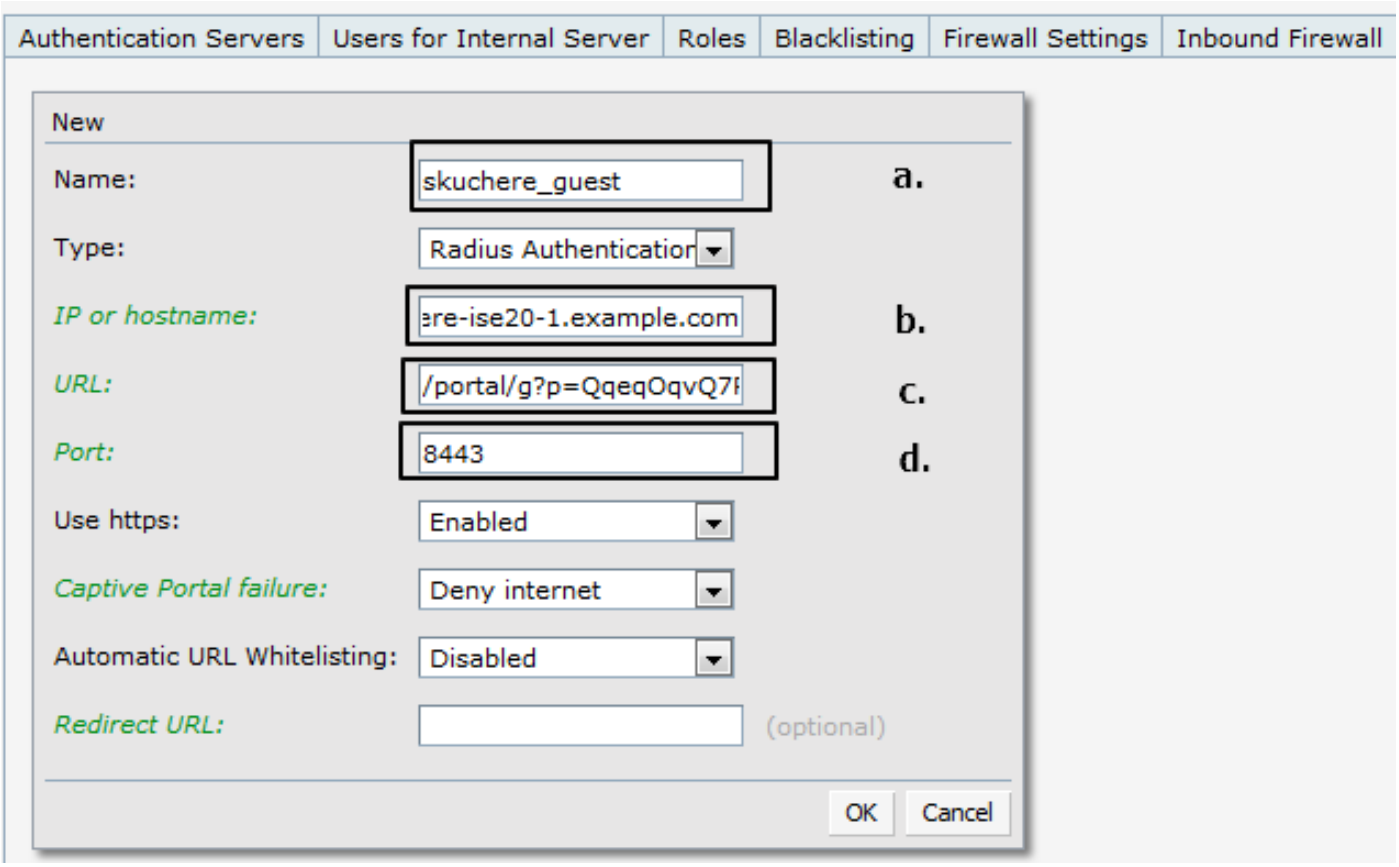
1. Choisissez le mécanisme de gestion des clés.
2. Définissez la clé pré-partagée.
3. Pour authentifier l'utilisateur contre ISE utilisant le besoin de filtrage MAC de MAB d'être activé.
4. Dans la liste de serveur d'authentification choisissez votre serveur d'AAA.

5. Pour activer la comptabilité vers le serveur précédemment défini d'AAA choisissez le serveur d'authentification d'utilisation dans la liste déroulante.

   Remarque: La comptabilité est cruciale avec la troisième-partie NADs. Si le noeud de service de stratégie (le RPC) ne reçoit pas le Comptabilité-arrêt pour l'utilisateur du NAD, la session peut être bloqué dans l'état commencé.

Étape 6. Configurez le portail captif.

Naviguez vers la **Sécurité > les portails captifs externes** et créez le nouveau portail, suivant les indications de l'image :



Étape 1. Spécifiez le nom portail captif.

Steo 2. définissent votre FQDN ISE ou adresse IP. Si vous utilisez l'adresse IP, assurez-vous que cet IP défini dans le domaine alternatif soumis de Name(SAN) du certificat portail d'invité.

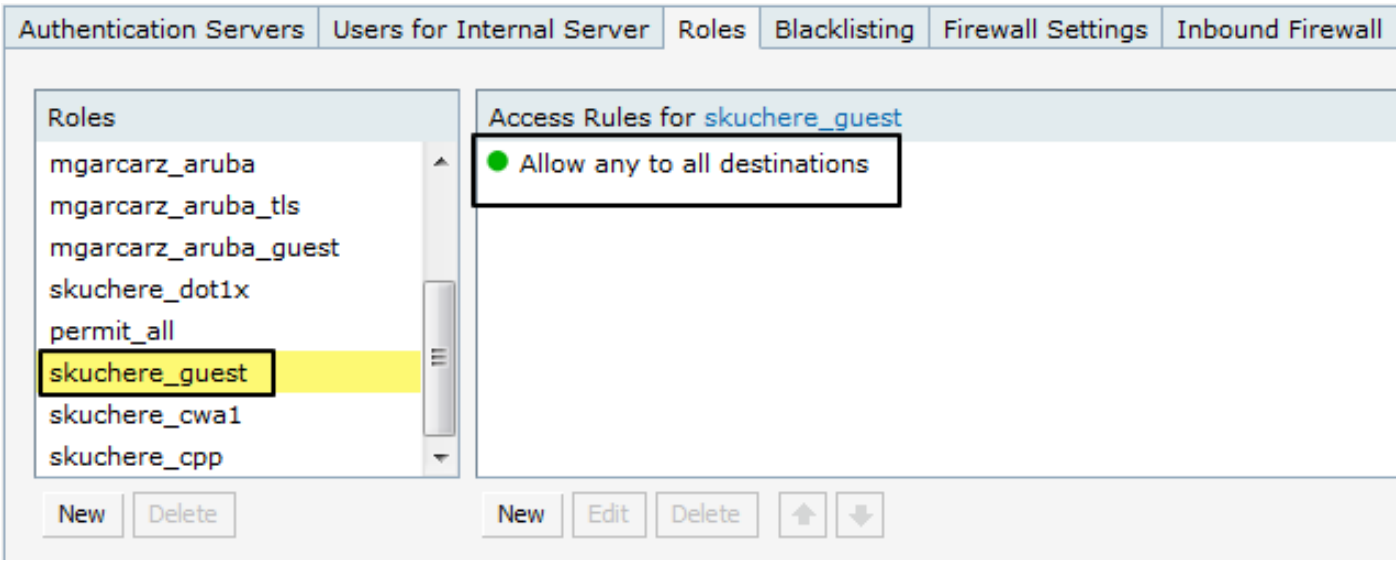
Remarque: Vous pouvez utiliser n'importe quel serveur RPC, mais l'utilisateur devrait être toujours réorienté au serveur où le MAB a eu lieu. Habituellement vous devez définir le FQDN du serveur de rayon qui a été configuré sur le SSID.

Étape 3. Provide réorientent du profil d'autorisation ISE. Vous devriez mettre ici la pièce après numéro de port,

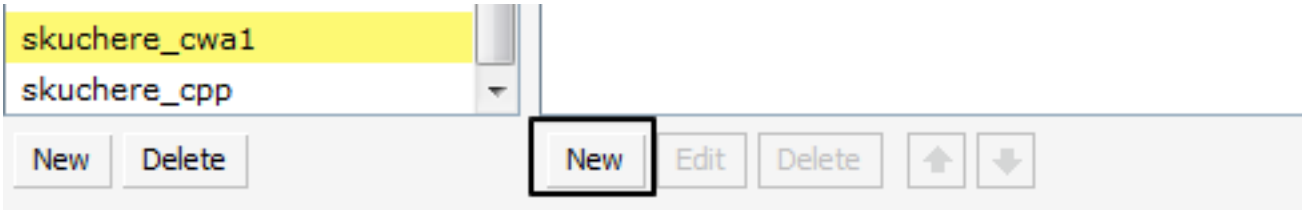
Étape 4. Définissez le port portail d'invité ISE.

Étape 7. Configurez les rôles de l'utilisateur.

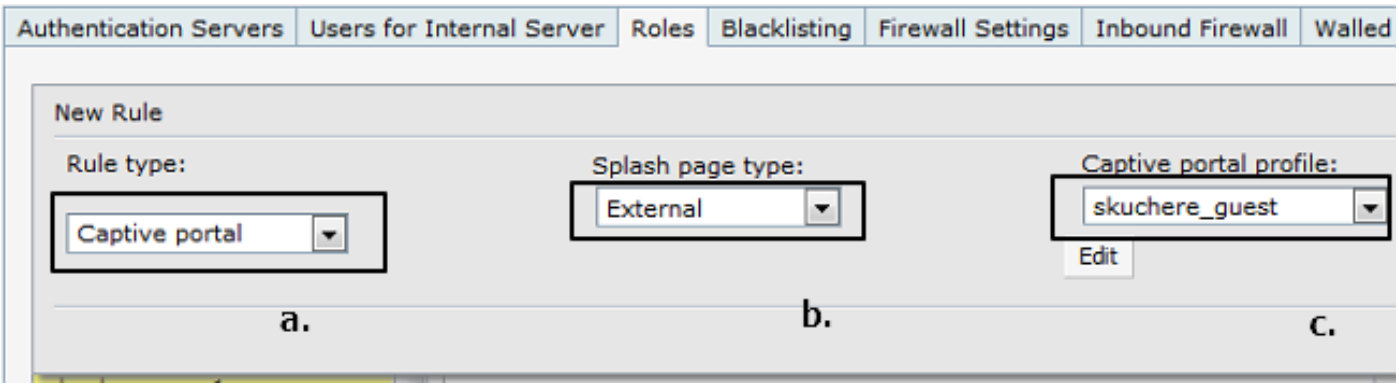
Naviguez vers la **Sécurité > les rôles.** Assurez-vous qu'après que le SSID soit créé, le nouveau rôle avec le même nom est présent dans la liste avec l'autorisation de règle d'accès à toutes les destinations. Supplémentaire, créez deux rôles : un pour CWA réorientent et en second lieu pour l'accès d'autorisation après authentification sur des portails d'invité. Les noms de ces rôles devraient être identiques au rôle de l'utilisateur d'Aruba défini dans des profils d'autorisation ISE.



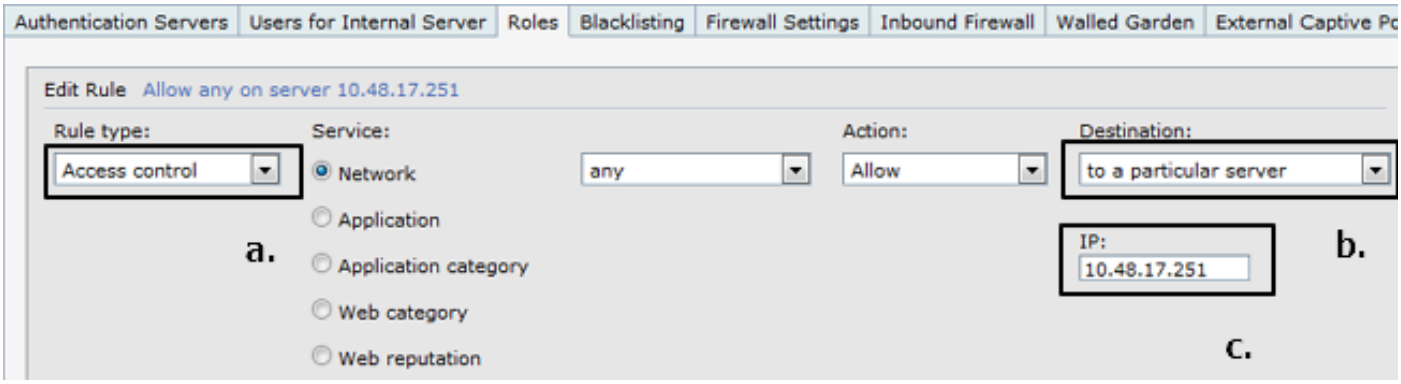
Suivant les indications de l'image, créez le nouveau rôle de l'utilisateur pour réorientent et ajoutent la restriction de Sécurité.



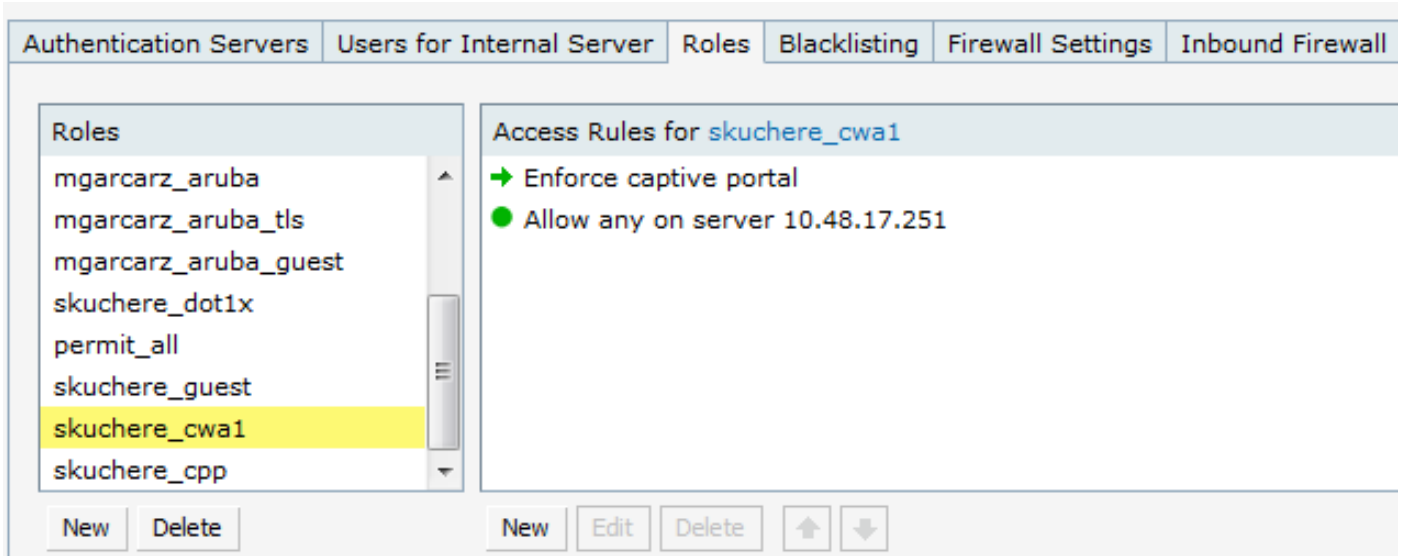
Pour la première restriction vous devez définir :



Pour la deuxième restriction vous devez définir :

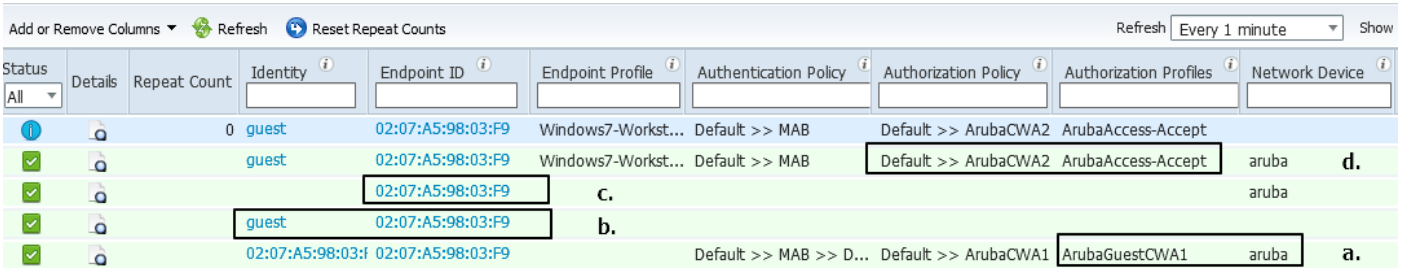


Suivant les indications de l'image, la règle par défaut en permettent à toutes les destinations peut être supprimée. C'est un résultat récapitulatif de configuration de rôle.



Vérifiez

Exemple d'écoulement d'invité dans les **exécutions > le rayon Livelog** ISE.



1. Le premier MAB et en conséquence, un profil d'autorisation avec CWA réorientent et rôle de l'utilisateur qui ont le portail captif configuré du côté d'Aruba.
2. Authentification d'invité.
3. Modification réussie de l'autorisation (CoA).
4. Deuxième MAB et en conséquence un profil d'autorisation avec l'accès et le rôle de l'utilisateur d'autorisation qui a l'autorisation toute la règle de côté d'Aruba.

Du côté d'Aruba vous pouvez utiliser des **clients d'exposition** commandez de s'assurer que l'utilisateur est connecté, adresse IP est assigné et corrige le rôle de l'utilisateur est assigné en raison de l'authentification :

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

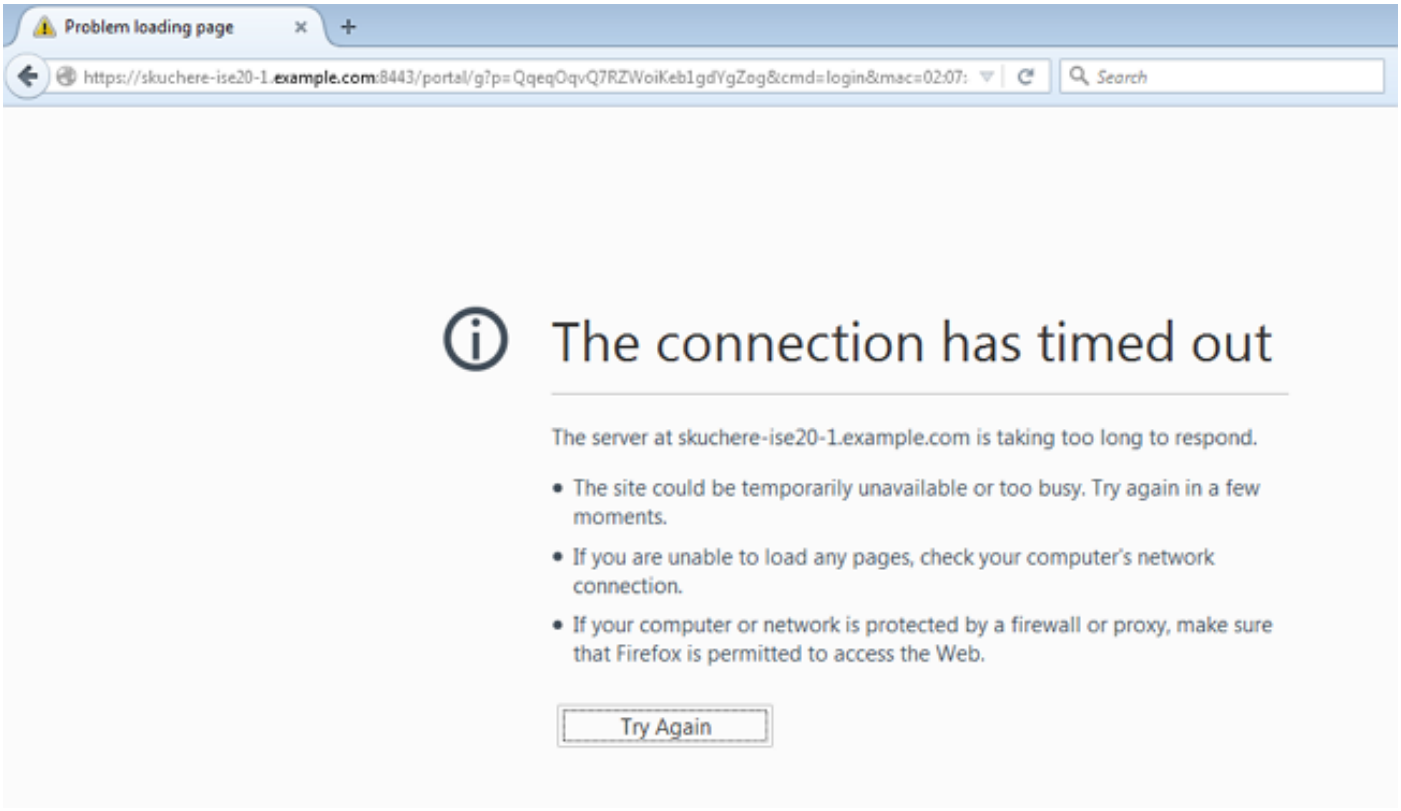
Dépannez

COA défectueux

Dans des configurations ISE, assurez-vous qu'Aruba NAD est configuré avec le type de périphérique de réseau approprié du côté ISE et port COA est correctement défini dans des configurations NAD. Du côté d'Aruba assurez-vous que RFC 3576 est activé dans des configurations de serveur d'authentification et port COA est défini correctement. Du contrôle de point de vue de réseau qu'on permet le port UDP 3799 entre ISE et Aruba WLC.

Réorientez la question

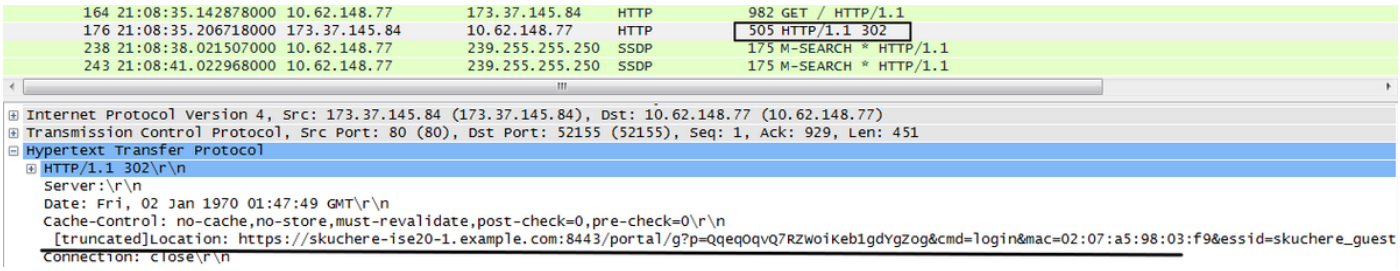
L'utilisateur voit l'URL ISE en navigateur mais la page ISE n'est pas affichée, suivant les indications de l'image :



Du côté utilisateur assurez-vous que le FQDN ISE peut être avec succès résolu pour corriger l'IP. Sur le contrôle latéral d'Aruba que l'URL ISE est défini correctement dans les configurations et le trafic portaiux captifs vers ISE permis dans le rôle de l'utilisateur de restrictions d'accès. Vérifiez également que le serveur de rayon sur le RPC SSID et ISE dans les configurations portailes captives est le même périphérique. Du contrôle de point de vue de réseau qu'on permet le port TCP 8443 du segment d'utilisateur à ISE.

Aucun présent URL de redirection en navigateur d'utilisateur

Du côté utilisateur assurez-vous que comme résultat de chaque demande de HTTP Aruba WLC renvoie la page du code 302 de HTTP déplacée avec l'URL ISE.



Le temporisateur piquant de session a expiré

Le symptôme typique de ce problème est que l'utilisateur est réorienté pendant la deuxième fois au portail d'invité. Dans ce cas dans le rayon Livelog ISE vous devriez voir cela après que le COA pour le deuxième profil d'autorisation d'authentification avec CWA ait été sélectionné de nouveau. Du côté d'Aruba, le rôle de l'utilisateur réel de contrôle avec l'aide des **clients d'exposition** commandent.

Comme un contournement pour cette question vous peut utiliser la stratégie d'autorisation basée par point final sur ISE pour des connexions après l'authentification réussie d'invité.