Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine

Contenu

Introduction

Ce document décrit comment configurer l'authentification Web centrale avec des clients câblés connectés aux Commutateurs à l'aide du Cisco Identity Services Engine (ISE).

Le concept de l'authentification Web centrale est opposé à l'authentification Web locale, qui est l'authentification Web habituelle sur le commutateur elle-même. Dans ce système, sur la panne dot1x/mab, le commutateur Basculement au profil de webauth et réorientera le trafic de client à une page Web sur le commutateur.

L'authentification Web centrale offre la possibilité pour avoir un périphérique central qui agit en tant que portail web (en Th est l'exemple, l'ISE). La difference majeure comparée à l'authentification Web locale habituelle est qu'elle est décalée pour poser 2 avec l'authentification mac/dot1x. Le concept diffère également parce que le serveur de rayon (ISE dans cet exemple) renvoie les attributs spéciaux qui indiquent au commutateur qu'une redirection de Web doit se produire. Cette solution a l'avantage pour éliminer n'importe quel retard qui était nécessaire pour que l'authentification Web donne un coup de pied. Globalement, si l'adresse MAC de la station client n'est pas connue par le serveur de rayon (mais d'autres critères peut également être utilisé),

les attributs de redirection de retours de serveur, et le commutateur autorise la station (par l'intermédiaire de contournement d'authentification MAC [MAB]) mais place une liste d'accès pour réorienter le trafic web au portail. Une fois l'utilisateur ouvre une session sur le portail d'invité, il est possible par l'intermédiaire de CoA (modification de l'autorisation) pour rebondir le port de commutateur de sorte qu'une nouvelle authentification de MAB de la couche 2 se produise. L'ISE peut alors se souvenir l'était un utilisateur de webauth et s'appliquer des attributs de la couche 2 (comme VAN assignment dynamique) à l'utilisateur. Un composant d'ActiveX peut également forcer le PC client pour régénérer son adresse IP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Identity Services Engine (ISE)
- Configuration de commutateur de Cisco IOS®

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco Identity Services Engine (ISE), version 1.1.1
- Commutateur de gamme Cisco Catalyst 3560 qui exécute la version de logiciel 12.2.55SE3

  Remarque: La procédure est semblable ou identique pour d'autres modèles de commutateur de Catalyst. Vous pouvez utiliser ces étapes sur toutes les versions du logiciel Cisco IOS pour le Catalyst sauf indication contraire.

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.

Configurez

Aperçu

La configuration ISE se compose de ces cinq étapes :

1. Créez la liste de contrôle d'accès téléchargeable (ACL).
2. Créez le profil d'autorisation.
3. Créez une règle d'authentification.
4. Créez une règle d'autorisation.
5. Activez le renouvellement IP (facultatif).

Créez l'ACL téléchargeable

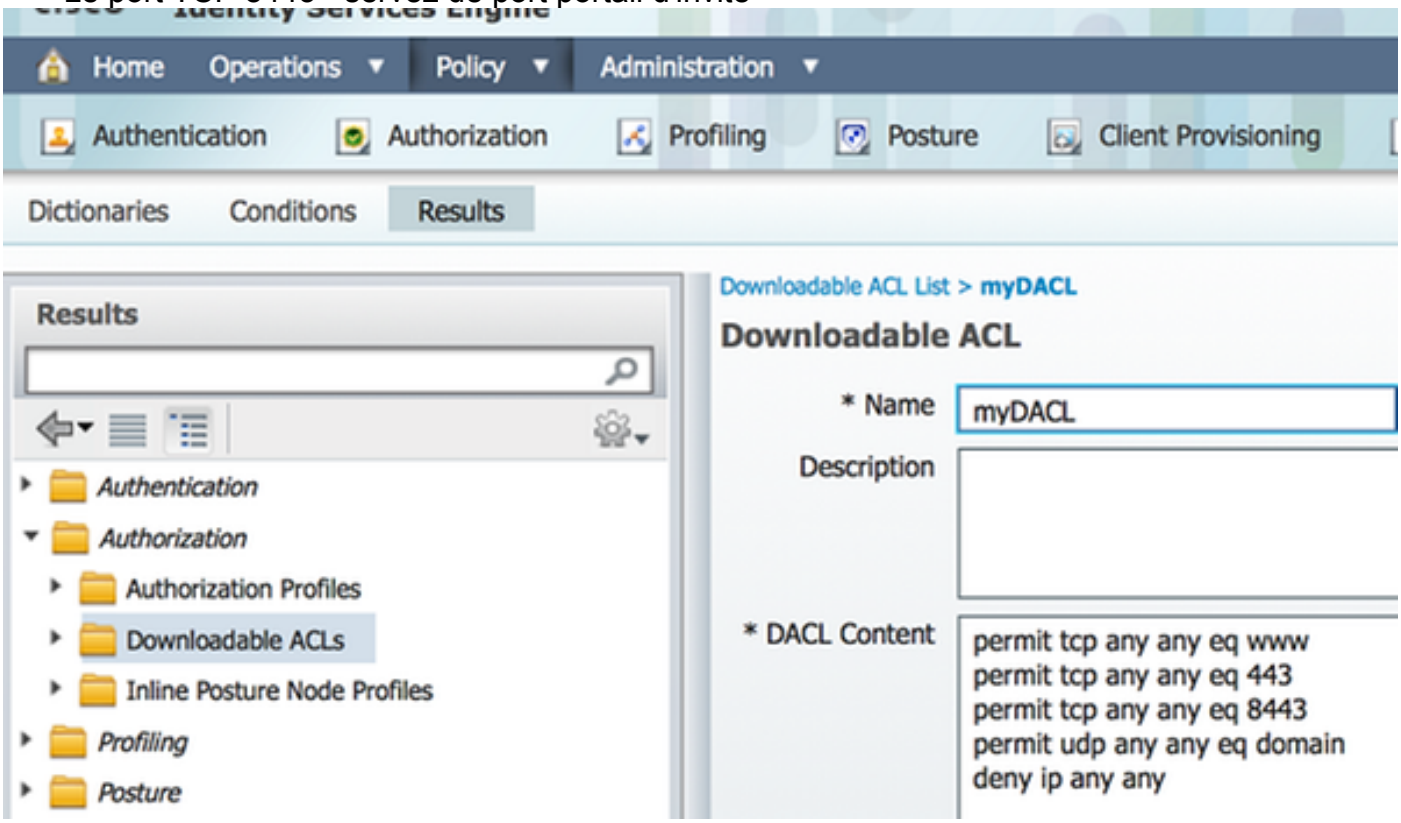
Ce n'est pas une étape obligatoire. L'ACL de réorientation renvoyé avec le profil central de webauth détermine ce que le trafic (HTTP ou HTTPS) est réorienté à l'ISE. L'ACL téléchargeable te permet pour définir quel trafic est permis. Vous devriez typiquement tenir compte des DN, des HTTPS, et de 8443 et refuser le repos. Autrement, le commutateur réoriente le trafic http mais permet d'autres protocoles.

Terminez-vous ces étapes afin de créer l'ACL téléchargeable :

1. **Stratégie de** clic, et **éléments de stratégie de** clic.
2. **Résultats de** clic.
3. Développez l'**autorisation**, et cliquez sur **ACLs téléchargeable**.
4. Cliquez sur le bouton d'**ajouter** afin de créer un nouvel ACL téléchargeable.
5. Dans la zone d'**identification**, écrivez un nom pour le DACL. Cet exemple utilise le *myDACL*.

Cette image affiche le contenu typique DACL, qui laisse :

- Des DN - résolvez l'adresse Internet de portail ISE
- HTTP et HTTPS - permettez la redirection
- Le port TCP 8443 - servez de port portail d'invité



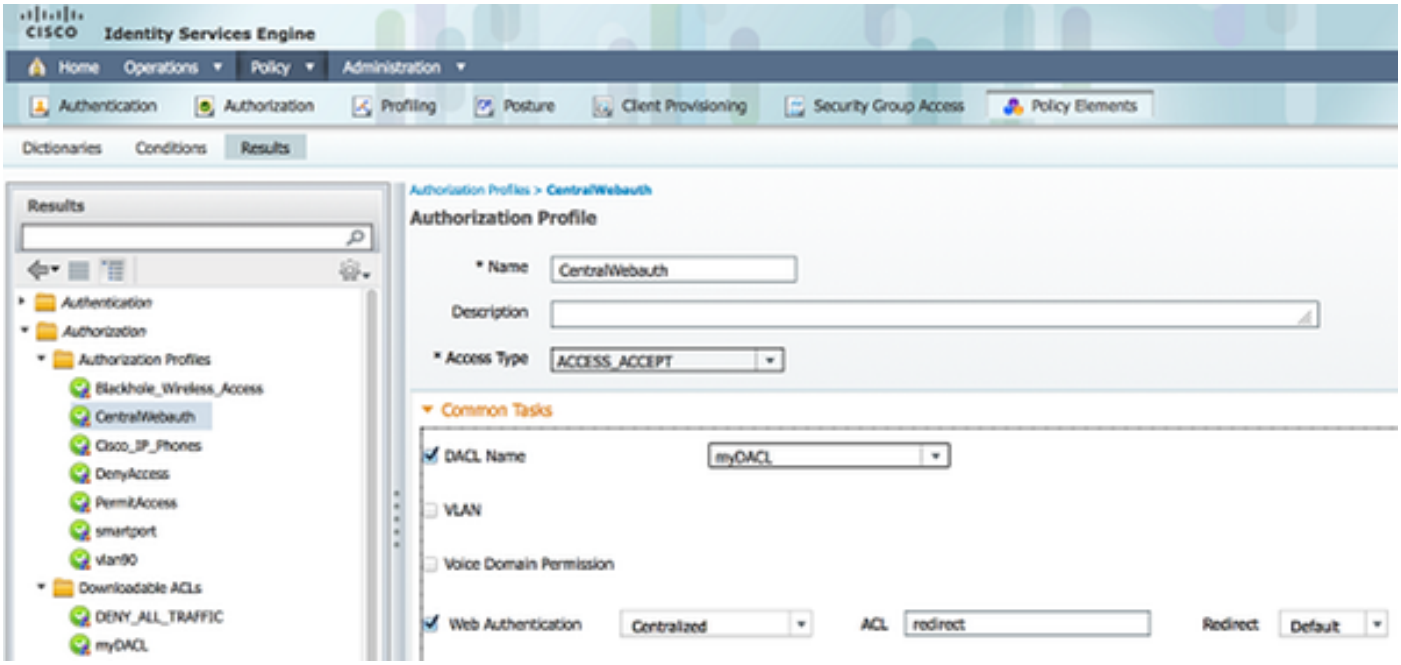
Créez le profil d'autorisation

Terminez-vous ces étapes afin de créer le profil d'autorisation :

1. **Stratégie de** clic, et **éléments de stratégie de** clic.
2. **Résultats de** clic.
3. Développez l'**autorisation**, et cliquez sur le **profil d'autorisation**.
4. Cliquez sur le bouton d'**ajouter** afin de créer un nouveau profil d'autorisation pour le webauth central.
5. Dans la zone d'**identification**, écrivez un nom pour le profil. Cet exemple utilise *CentralWebauth*.

6. Choisissez **ACCESS_ACCEPT de la** liste déroulante de type d'Access.
7. Cochez la case d'**authentification Web**, et choisissez **centralisé de la** liste déroulante.
8. Dans le domaine d'ACL, écrivez le nom de l'ACL sur le commutateur qui définit le trafic à réorienter. Ce les exemples les utilise *réorientent*.
9. Choisissez le **par défaut de la** liste déroulante de réorientation.
10. Vérifiez la case à cocher de **nom DACL**, et choisissez le **myDACL du** lsit de déroulant si vous décidez d'utiliser un DACL au lieu d'un ACL de prise de pression statique sur le commutateur.

L'attribut de réorientation définit si l'ISE voit le portail de web par défaut ou un portail web fait sur commande que l'admin ISE a créés. Par exemple, l'ACL de *réorientation* dans cet exemple déclenche une redirection sur le trafic de HTTP ou HTTPS du client à n'importe où. L'ACL est défini sur le commutateur plus tard dans cet exemple de configuration.

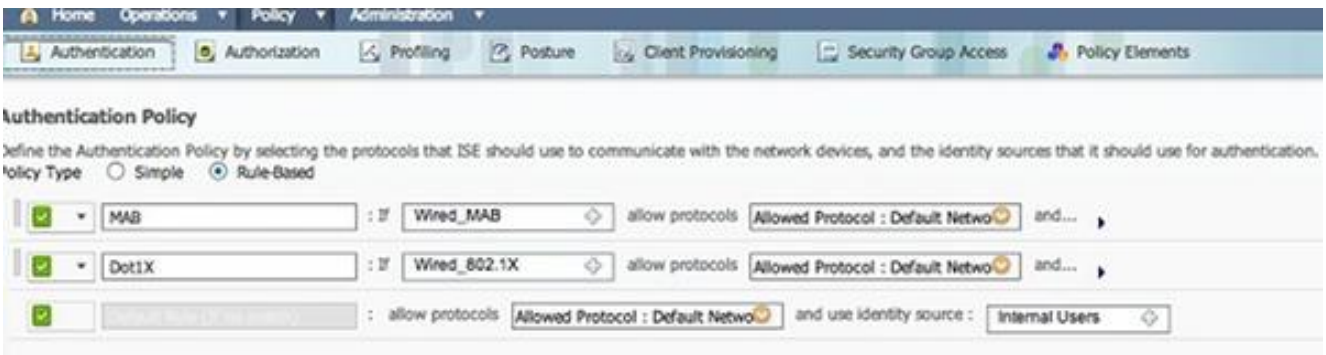


Créez une règle d'authentification

Terminez-vous ces étapes afin d'employer le profil d'authentification pour créer la règle d'authentification :

1. Sous le menu de stratégie, **authentification de** clic.

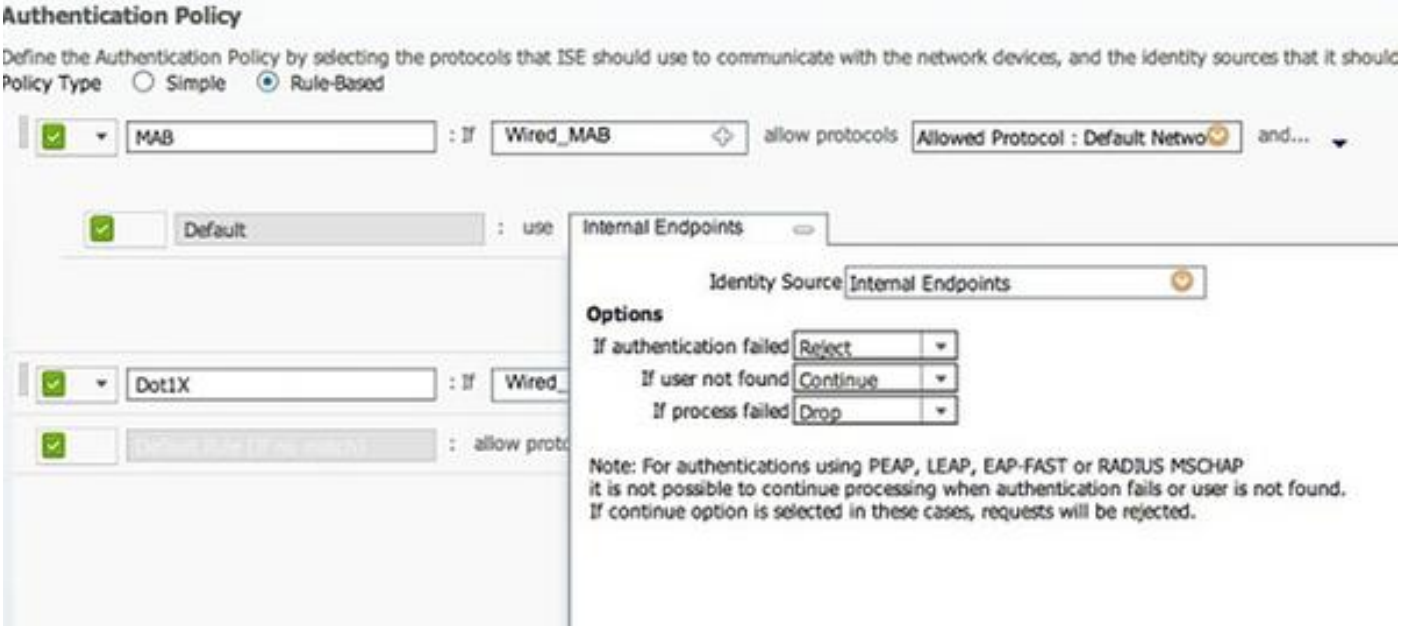
   Cette image affiche un exemple de la façon configurer la règle de stratégie d'authentification. Dans cet exemple, on configure une règle qui déclenche quand le MAB est détecté.



2. Écrivez un nom pour votre règle d'authentification. Cet exemple utilise le *MAB*.

3. Sélectionnez (**+**) l'icône plus dans si champ de condition.
4. Choisissez l'**état composé**, et choisissez **Wired_MAB**.
5. Cliquez sur la flèche localisée à côté de **et…** afin de développer la règle plus loin.
6. Cliquez sur **+** icône dans le domaine de source d'identité, et choisissez les **points finaux internes**.
7. Choisissez **continuent du** « si liste déroulante non trouvée d'utilisateur ».

   Cette option permet un périphérique à authentifier (par le webauth) même si son adresse MAC n'est pas connue. Les clients de dot1x peuvent encore authentifier avec leurs qualifications et ne devraient pas être concernés par cette configuration.



Créez une règle d'autorisation

Il y a maintenant plusieurs règles de configurer dans la stratégie d'autorisation. Quand le PC est branché, il passe par le MAB ; on le suppose que l'adresse MAC n'est pas connue, ainsi le webauth et l'ACL sont retournés. Cette règle *non connue de MAC* est affichée dans cette image et est configurée dans cette section :

Terminez-vous ces étapes afin de créer la règle d'autorisation :

1. Créez une nouvelle règle, et écrivez un nom. Cet exemple utilise le *MAC non connu*.
2. Cliquez sur (**+**) l'icône plus dans le domaine de condition, et choisissez de créer un nouvel état.
3. Développez la liste déroulante d'**expression**.
4. Choisissez l'**accès au réseau**, et développez-le.
5. Cliquez sur **AuthenticationStatus**, et choisissez l'opérateur d'**égaux**.
6. Choisissez **UnknownUser** dans le domaine droit.
7. Àla page générale d'autorisation, choisissez **CentralWebauth** (profil d'autorisation) dans le domaine à la droite du mot *alors*.

Cette étape permet à l'ISE pour continuer quoique l'utilisateur (ou le MAC) ne soit pas connu.

Des utilisateurs inconnus sont maintenant présentés avec la page de connexion. Cependant, une fois qu'ils entrent dans leurs qualifications, ils sont présentés de nouveau avec une demande d'authentification sur l'ISE ; donc, une autre règle doit être configurée avec une condition qui est remplie si l'utilisateur est un utilisateur d'invité. Dans cet exemple, *si l'invité d'égaux d'UseridentityGroup* est utilisé, et lui est supposé que tous les invités appartiennent à ce groupe.

8. Cliquez sur les actions se boutonnent situé à la fin de la règle *non connue de MAC*, et choisissent d'insérer une nouvelle règle ci-dessus.

   Remarque: Il est très important que cette nouvelle règle soit livré avant que la règle *non connue de MAC*.
9. Écrivez un nom pour la nouvelle règle. Cet exemple utilise l'Être-un-*INVITÉ*.
10. Choisissez une condition qui apparie vos utilisateurs d'invité.

    Cet exemple utilise *InternalUser : IdentityGroup égale l'invité* parce que tous les utilisateurs d'invité sont liés à un groupe d'*invité* (ou à un groupe différent que vous avez configuré dans vos configurations de sponsor).
11. Choisissez **PermitAccess** dans la case de résultat (située à la droite du mot *puis*).

    Quand l'utilisateur est autorisé sur la page de connexion, ISE redémarre une authentification de la couche 2 sur le port de commutateur, et un nouveau MAB se produit. Dans ce scénario, la différence est qu'un indicateur invisible est placé pour qu'ISE se souvienne que c'était un utilisateur invité-authentifié. Cette règle est la *2ème AUTHENTIQUE*, et la condition est *accès au réseau : UseCase égale GuestFlow*. Cette condition est remplie quand l'utilisateur authentifie par l'intermédiaire du webauth, et le port de commutateur est placé de nouveau pour un nouveau MAB. Vous pouvez assigner tous les attributs que vous aimez. Cet exemple assigne un profil *vlan90* de sorte que l'utilisateur soit assigné le VLAN 90 dans sa deuxième authentification de MAB.
12. Cliquez sur les **actions** (situées à la fin de la règle d'Être-un-INVITÉ), et choisissez la **nouvelle règle d'insertion ci-dessus**.
13. Entrez dans le **2ème AUTHENTIQUE** dans la zone d'identification.
14. Dans le domaine de condition, cliquez sur (**+**) l'icône plus, et choisissez de créer un nouvel état.
15. Choisissez l'**accès au réseau**, et cliquez sur **UseCase**.
16. Choisissez les **égaux** en tant qu'opérateur.
17. Choisissez **GuestFlow** comme bon opérande.
18. Àla page d'autorisation, cliquez sur (**+**) l'icône plus (située à côté de *puis*) afin de choisir un résultat pour votre règle.

    Dans cet exemple, un profil préconfiguré (vlan90) est assigné ; cette configuration n'est pas affichée dans ce document.

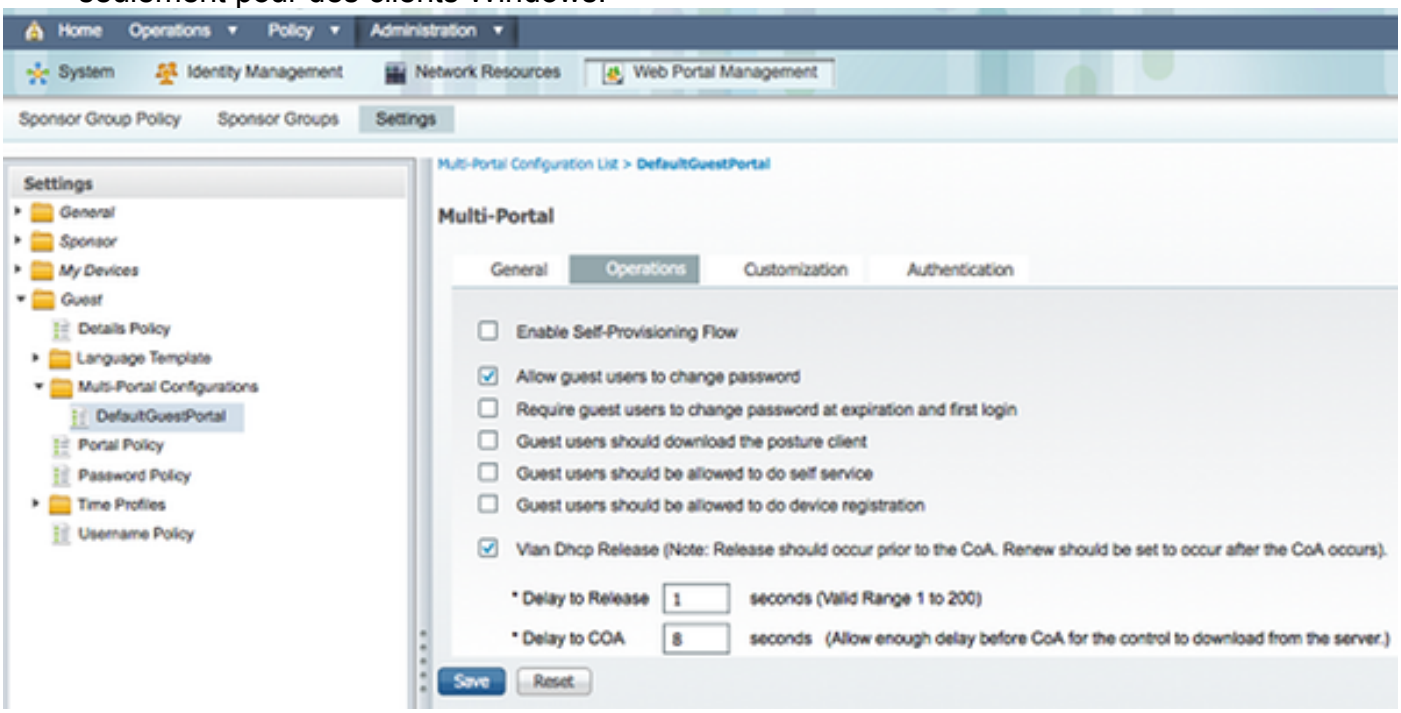
    Vous pouvez choisir une option d'**Access d'autorisation** ou créer un profil fait sur commande afin de renvoyer le VLAN ou les attributs ces vous aimez.

Activez le renouvellement IP (facultatif)

Si vous assignez un VLAN, la dernière étape est pour que le PC client renouvelle son adresse IP. Cette étape est réalisée par le portail d'invité pour des clients Windows. Si vous ne placiez pas un VLAN pour la *2ème* règle *AUTHENTIQUE* plus tôt, vous pouvez ignorer cette étape.

Si vous assigniez un VLAN, terminez-vous ces étapes afin d'activer le renouvellement IP :

1. **Gestion de** clic, et **Gestion d'invité de** clic.
2. **Configurations de** clic.
3. Développez l'**invité**, et développez la **configuration Multi-portaile**.
4. Clic **DefaultGuestPortal** ou le nom d'un portail fait sur commande que vous avez pu avoir créé.
5. Cliquez sur la case **DHCP Releasecheck de VLAN**. Remarque: Cette option fonctionne seulement pour des clients Windows.



Commutez la configuration (l'extrait)

Cette section fournit un extrait de la configuration de commutateur. Voir la configuration de commutateur (pleine) pour la configuration complète.

Cet échantillon affiche une configuration simple de MAB.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 100 est le VLAN qui fournit la pleine connexion réseau. Un ACL par défaut de port (*webauth*

Désigné) est appliqué et défini en tant qu'affiché ici :

```
ip access-list extended webauth
permit ip any any
```

Cette configuration d'échantillon donne le plein accès au réseau même si l'utilisateur n'est pas authentifié ; donc, vous pourriez vouloir limiter l'accès aux utilisateurs unauthenticated.

Dans cette configuration, le HTTP et le HTTPS parcourant ne fonctionne pas sans authentification (par l'autre ACL) puisqu'ISE est configuré pour utiliser un ACL de réorientation (nommé *réorientez*). Voici la définition sur le commutateur :

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

Cette liste d'accès doit être définie sur le commutateur afin de définir sur quel trafic le commutateur exécutera la redirection. (Il s'assortit sur l'*autorisation*.) Dans cet exemple, tout trafic de HTTP ou HTTPS que le client envoie des déclencheurs à une redirection de Web. Cet exemple refuse également l'adresse IP ISE ainsi le trafic à l'ISE va à l'ISE et ne réoriente pas dans une boucle. (Dans ce scénario, refusez ne bloque pas le trafic ; il juste ne réoriente pas le trafic.) Si vous utilisez des ports HTTP peu communs ou un proxy, vous pouvez ajouter d'autres ports.

Une autre possibilité est de permettre l'accès HTTP à quelques sites Web et de réorienter d'autres sites Web. Par exemple, si vous définissez dans l'ACL une autorisation pour des web server internes seulement, les clients pourraient parcourir le Web sans authentifier mais rencontreraient la réorientation s'ils essayent d'accéder à un web server interne.

La dernière étape est de permettre le CoA sur le commutateur. Autrement, l'ISE ne peut pas forcer le commutateur pour authentifier à nouveau le client.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

Cette commande est exigée pour que le commutateur réoriente basé sur le trafic http :

```
ip http server
```

Cette commande est exigée pour réorienter basé sur le trafic HTTPS :

```
ip http secure-server
```

Ces commandes sont également importantes :

```
radius-server vsa send authentication
radius-server vsa send accounting
```

Si l'utilisateur n'est pas encore authentifié, le **num> de <interface de la session international de show authentication** renvoie cette sortie :

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
```

```
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Remarque: En dépit d'une authentification réussie de MAB, l'ACL de réorientation est placé puisque l'adresse MAC n'a pas été connue par l'ISE.

Commutez la configuration (pleine)

Cette section répertorie la configuration de plein commutateur. Quelques interfaces et lignes de commande inutiles ont été omises ; donc, cette configuration d'échantillon devrait être utilisée pour la référence seulement et ne devrait pas être copiée.

```
Building configuration...

Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
```

```
vtp interface Vlan61
udld enable

nmsp enable
ip routing
ip dhcp binding cleanup interval 600
!
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsakeypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
```

```
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
!
ip sla enable reaction-alerts
logging esm config
logging trap warnings
logging facility auth
logging 10.48.76.31
snmp-server community c3560public RO
snmp-server community c3560private RW
snmp-server community private RO
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send authentication
radius-server vsa send accounting
!
!
!
privilege exec level 15 configure terminal
privilege exec level 15 configure
privilege exec level 2 debug radius
privilege exec level 2 debug aaa
privilege exec level 2 debug
!
line con 0
line vty 0 4
exec-timeout 0 0
password Cisco123
authorization commands 1 MyTacacs
authorization commands 2 MyTacacs
authorization commands 15 MyTacacs
authorization exec MyTacacs
login authentication MyTacacs
line vty 5 15
!
ntp server 10.48.76.33
end
```

Configuration de proxy HTTP

Si vous utilisez un proxy HTTP pour vos clients, il signifie que vos clients :

- Utilisez un port peu conventionnel pour le protocole HTTP
- Envoyez tout leur trafic à ce proxy

Afin de faire écouter le commutateur sur le port peu conventionnel (par exemple, 8080), utilisez ces commandes :

```
ip http port 8080
ip port-map http port 8080
```

Vous devez également configurer tous les clients pour continuer à utiliser leur proxy mais pour ne pas utiliser le proxy pour l'adresse IP ISE. Tous les navigateurs incluent une caractéristique qui te permet pour écrire les noms d'hôte ou les adresses IP qui ne devraient pas utiliser le proxy. Si vous n'ajoutez pas l'exception pour l'ISE, vous rencontrez une page d'authentification de boucle.

Vous devez également modifier votre ACL de redirection pour autoriser sur le port de proxy (8080 dans cet exemple).

L'information importante au sujet du commutateur SVI

Àce moment, le commutateur a besoin d'une interface virtuelle de commutateur (SVI) afin de répondre au client et envoyer la redirection de portail web au client. Ce SVI ne doit pas nécessairement être sur le client subnet/VLAN. Cependant, si le commutateur n'a aucun SVI dans le client subnet/VLAN, il doit utiliser l'un des d'autres SVI et envoyer le trafic comme défini dans la table de routage de client. Ceci signifie typiquement que le trafic est envoyé à une autre passerelle au centre du réseau ; ce trafic revient au commutateur d'accès à l'intérieur du sous-réseau de client.

De Pare-feu le trafic de bloc typiquement et derrière le même commutateur, comme dans ce scénario, ainsi la redirection ne pourrait pas fonctionner correctement. Les contournements sont de permettre ce comportement sur le Pare-feu ou de créer un SVI sur le commutateur d'accès dans le sous-réseau de client.

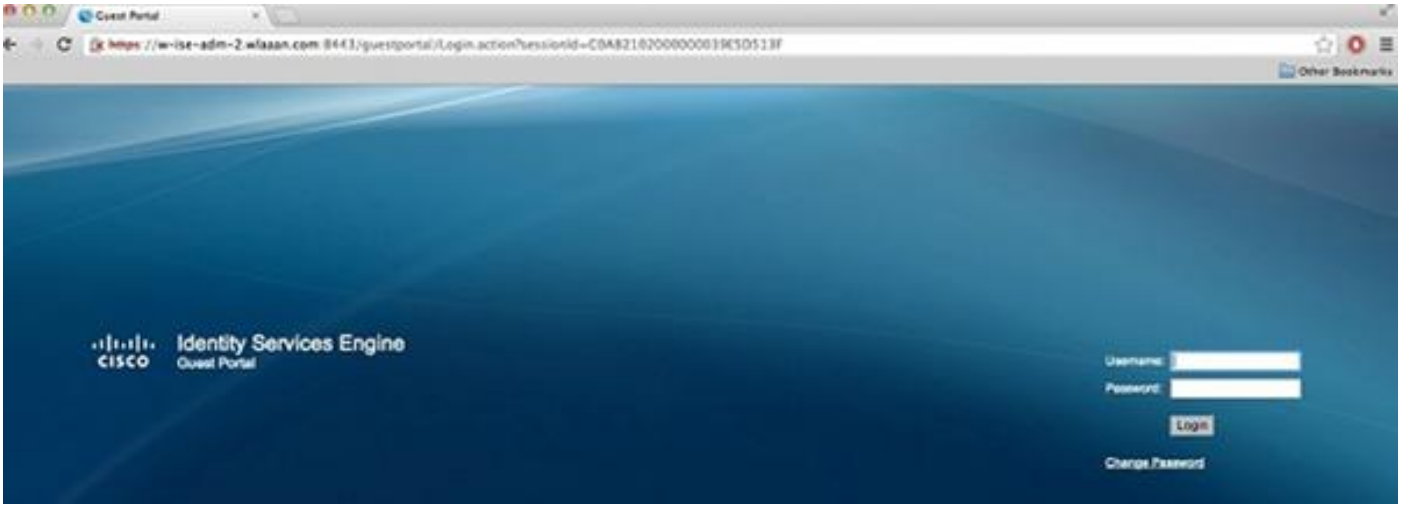
L'information importante au sujet de la redirection HTTPS

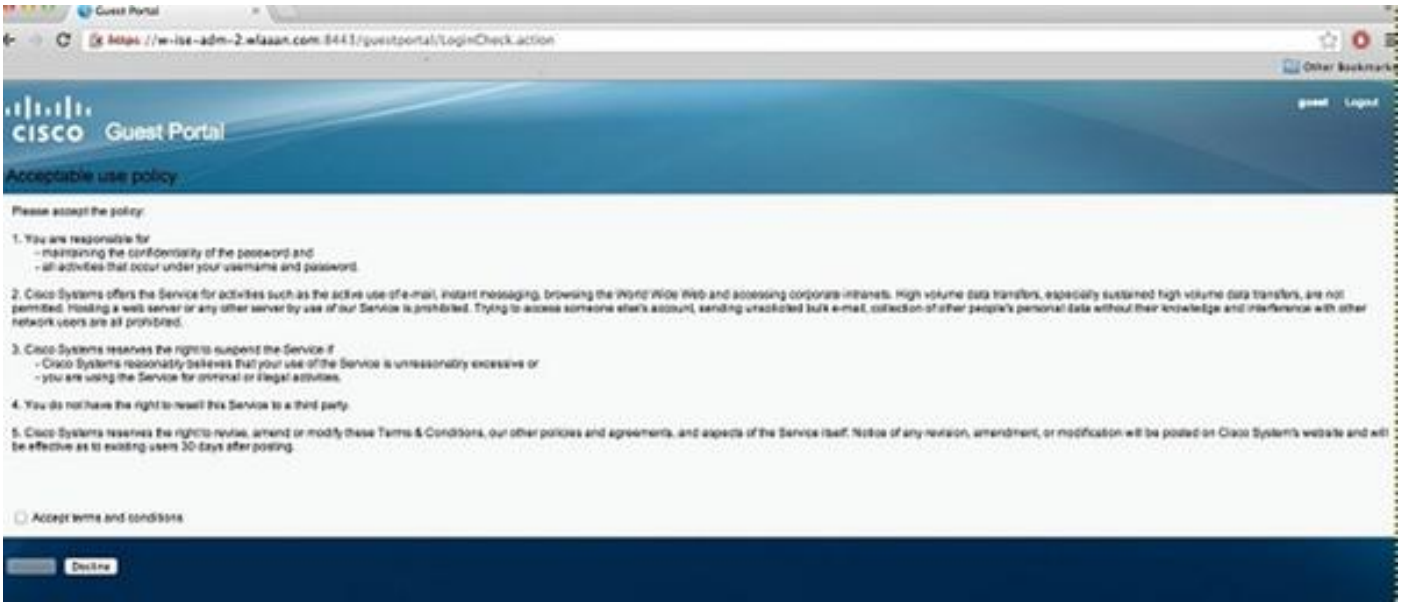
Les Commutateurs peuvent réorienter le trafic HTTPS. Ainsi, si le client d'invité a une page d'accueil dans HTTPS, la redirection se produit correctement.

Le concept entier de la redirection est basé sur le fait qu'un périphérique (dans ce cas, le commutateur) charrie l'adresse IP de site Web. Cependant, un problème crucial surgit quand le commutateur intercepte et réoriente le trafic HTTPS parce que le commutateur peut présenter seulement son propre certificat dans la prise de contact de Transport Layer Security (TLS). Puisque ce n'est pas le même certificat que le site Web initialement demandé, la plupart de commandant de question de navigateurs alerte. Les navigateurs manipulent correctement la redirection et la présentation d'un autre certificat comme problème de sécurité. Il n'y a aucun contournement pour ceci, et il n'y a aucune manière pour que le commutateur charrie votre certificat d'origine de site Web.

Résultat final

Le PC client branche et exécute le MAB. L'adresse MAC n'est pas connue, ainsi ISE pousse les attributs de redirection de nouveau au commutateur. Les essais d'utilisateur à aller à un site Web et est réorientés.

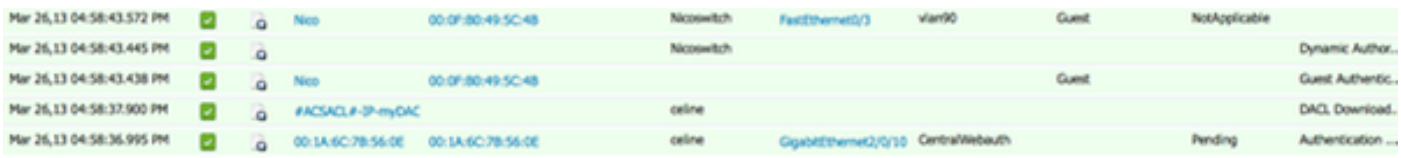




Quand l'authentification de la page de connexion est réussie, l'ISE rebondit le switchport par la modification de l'autorisation, qui reprend une authentification de MAB de la couche 2.

Cependant, l'ISE sait que c'est un ancien client de webauth et autorise le client basé sur les qualifications de webauth (bien que c'est une authentification de la couche 2).

Dans les logs d'authentification ISE, l'authentification de MAB apparaît au bas du log. Bien qu'il soit inconnu, l'adresse MAC a été authentifiée et profilée, et les attributs de webauth ont été retournés. Ensuite, l'authentification se produit avec le nom d'utilisateur de l'utilisateur (c'est-à-dire, les types d'utilisateur ses qualifications dans la page de connexion). Juste après l'authentification, une nouvelle authentification de la couche 2 se produit avec le nom d'utilisateur comme qualifications ; cette étape d'authentification est où vous pouvez retourner attribue un tel VLAN dynamique.



Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Logiciel Cisco Identity Services Engine
- Guide de référence des commandes de Logiciel Cisco Identity Services Engine
- Intégration d'ISE (Cisco Identity Services Engine) avec le Cisco WLC (contrôleur LAN Sans fil)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems