Configuration de la journalisation d'URL intégrée et du rapport du trafic hôte dans un réseau Cisco

Contenu

Introduction

Ce document décrit comment intégrer un NAC Guest Server (NGS) avec des contrôleurs LAN Sans fil (WLCs) et une appliance de sécurité adaptable (ASA) pour fournir l'URL se connectant et signalant du trafic d'invité. Beaucoup de sociétés ont une condition requise de surveiller le trafic d'invité, et ce document fournit des informations sur la façon dont configurer les composants de Cisco pour répondre à cette exigence.

Notez qu'il y a de plusieurs solutions de Cisco pour configurer l'accès invité dans un réseau de Cisco. Cet article se concentre sur la méthode qui utilise le WLC comme technologie de activation. Le WLC a la faculté unique au trafic du tunnel de la frontière du réseau à l'Internet avec EoIP. Cette caractéristique élimine la nécessité de déployer des VPN ou ACLs dans l'infrastructure réseau pour limiter le trafic d'invité de la fuite dans le réseau interne de la société.

La partie de cet article couvre « URL intégré se connectant et signalant » dans un réseau de « radio-invité », mais cette caractéristique peut être configurée dans un réseau de « câbler-invité », aussi bien. L'annexe A fournit des détails pour un réseau de « câbler-invité ».

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- ASA qui exécute la version 8.0.4.24 ou ultérieures
- Deux contrôleurs de la gamme WLC-4400 qui exécutent la version 4.2.130 ou ultérieures
- NAC Guest Server qui exécute la version 2.0 ou ultérieures

Composants utilisés

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

- ASA qui passages 8.0.4.26
- Deux contrôleurs WLC-44xx qui exécutent le code 4.2.130
- Serveur d'invité NAC qui exécute le code 2.0.0
- Catalyst 6500

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.

Conventions

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

Informations générales

L'accès invité sans fil fournit les avantages pour l'entreprise significatifs aux clients. Ces avantages incluent des coûts d'exploitation réduits, productivité améliorée, et Gestion et ravitaillement simplifiés d'accès invité. En outre, le NAC Guest Server permet à des clients d'afficher leur Acceptable Use Policy et d'avoir besoin de l'acceptation de cette stratégie avant d'accorder l'accès à Internet. Maintenant, en plus de l'URL intégré se connectant et signalant, les clients peuvent se connecter l'utilisation d'invité et la conformité de piste contre leur Acceptable Use Policy.

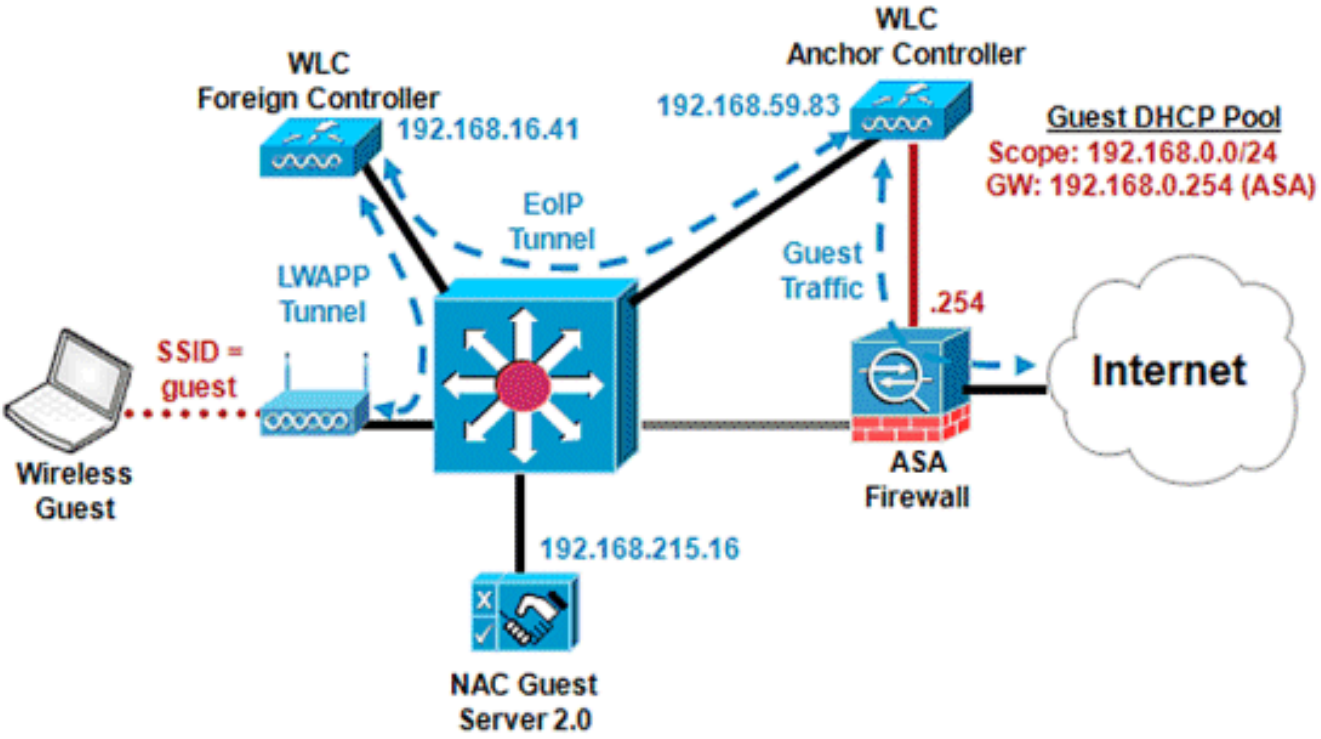
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Topologie de travaux pratiques de Radio-invité

Le Catalyst 6500 est utilisé pour simuler le réseau d'entreprise. L'invité SSID, affiché en rouge, trace au VLAN indigène à l'ASA, également affichée en rouge. La circulation d'invité du PC dans le Point d'accès, par le tunnel LWAPP au contrôleur étranger WLC, et puis par le tunnel d'EoIP au contrôleur d'ancre WLC. Le contrôleur d'ancre fournit le DHCP et les services d'authentification pour le réseau d'invité. Le service DHCP fournit à l'invité une adresse IP, une passerelle par défaut, et un serveur DNS. La passerelle par défaut est l'ASA, et le serveur DNS est un serveur public situé sur l'Internet. Le service d'authentification dans le contrôleur d'ancre communique avec le NGS par le RAYON pour authentifier des utilisateurs contre la base de données utilisateur d'invité dans le NGS. La connexion d'invité est initiée quand l'invité ouvre un navigateur Web, et le contrôleur d'ancre réoriente le trafic à la page d'authentification. Tout le trafic dans et hors du sous-réseau d'invité est filtré à l'aide de l'ASA pour le contrôle et auditer de stratégie.

URL intégré se connectant de l'ASA à NGS

Se connecter intégré URL est lancé quand vous activez ces derniers :

- Comptabilité de RAYON du contrôleur d'ancre WLC au NGS
- Se connecter du HTTP obtiennent des demandes dans l'ASA
- Envoi des messages de Syslog de l'ASA au NGS

La comptabilité de RAYON fournit au NGS un mappage entre l'adresse IP d'invité et l'user-id d'invité pendant une période spécifique. Se connecter du HTTP obtiennent des demandes fournit au NGS un log de quel URL a été visité par l'adresse IP d'invité quand. Le NGS peut alors corréler ces informations pour produire un état qui affiche l'URLs visité par un invité particulier pendant un délai prévu particulier.

Notez que le temps précis est exigé pour que cette corrélation fonctionne correctement. Pour cette raison, la configuration des serveurs de NTP est fortement recommandée sur l'ASA, le WLC, et le

NGS.

Configurations

Ce document utilise les configurations suivantes :

- Configuration ASA
- Configuration WLC
- Configuration NGS

Configuration ASA

Les tâches principales de configuration sur l'ASA incluent ces derniers :

- NTP
- Inspection de HTTP
- Syslog

Le NTP est exigé pour assurer la corrélation appropriée des messages par le NGS. L'inspection de HTTP active se connecter URL. Le Syslog est la méthode utilisée pour envoyer les logs URL au NGS.

Dans cet exemple, cette commande est utilisée d'activer le NTP sur l'ASA :

```
ntp server 192.168.215.62
```

L'inspection de HTTP permet à l'ASA de se connecter l'URLs. Spécifiquement, les commandes enables de **HTTP d'examiner** ou se connecter de débronchements de la demande GET avec le message 304001 de Syslog.

La commande de **HTTP d'examiner** est placée sous un class-map dans un policy-map. Une fois activés avec la commande de service-**stratégie**, les logs d'inspection de HTTP obtiennent des demandes avec le message 304001 de Syslog. Le code 8.0.4.24 ASA ou plus tard est exigé pour le message 304001 de Syslog pour afficher l'adresse Internet en tant qu'élément de l'URL.

Dans cet exemple, ce sont les commandes appropriées :

```
policy-map global_policy
 class inspection_default
  inspect http
!
service-policy global_policy global
```

Le Syslog est la méthode utilisée pour communiquer l'URL se connectant au NGS. Dans cette configuration, seulement le message 304001 de Syslog est envoyé au NGS avec cette configuration :

```
logging enable
logging timestamp
logging list WebLogging message 304001
logging trap WebLogging
logging facility 21
logging host inside 192.168.215.16
```

Configuration WLC

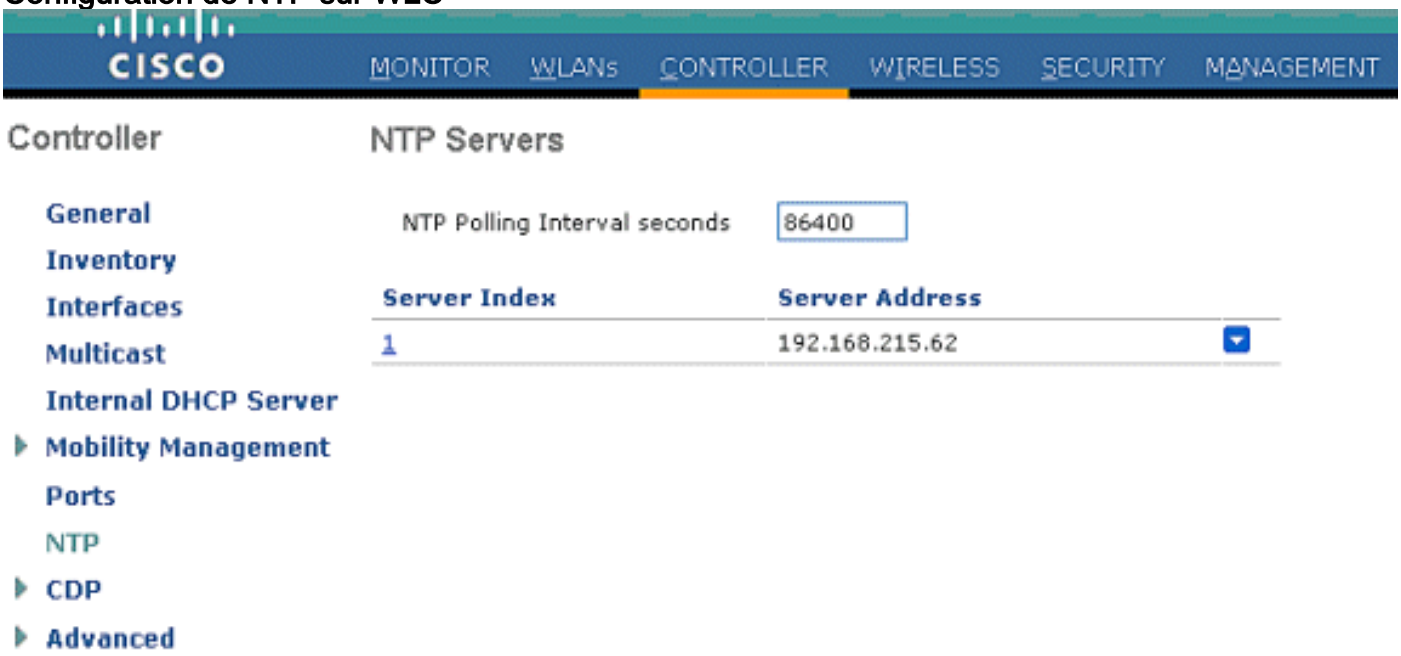
Les étapes principales de configuration pour les contrôleurs LAN Sans fil incluent ces derniers :

- Accès invité de base
- NTP
- Gestion des comptes RADIUS

La configuration de base d'accès invité implique la configuration d'un contrôleur étranger de contrôleur WLC et d'ancre WLC de sorte que le trafic d'invité soit percé un tunnel par le réseau d'entreprise à l'Internet DMZ. La configuration de l'accès invité de base est couverte dans la documentation distincte. Des illustrations qui affichent la configuration pour l'installation sont couvertes dans l'annexe.

Des serveurs de NTP sont ajoutés à l'écran Controller/NTP.

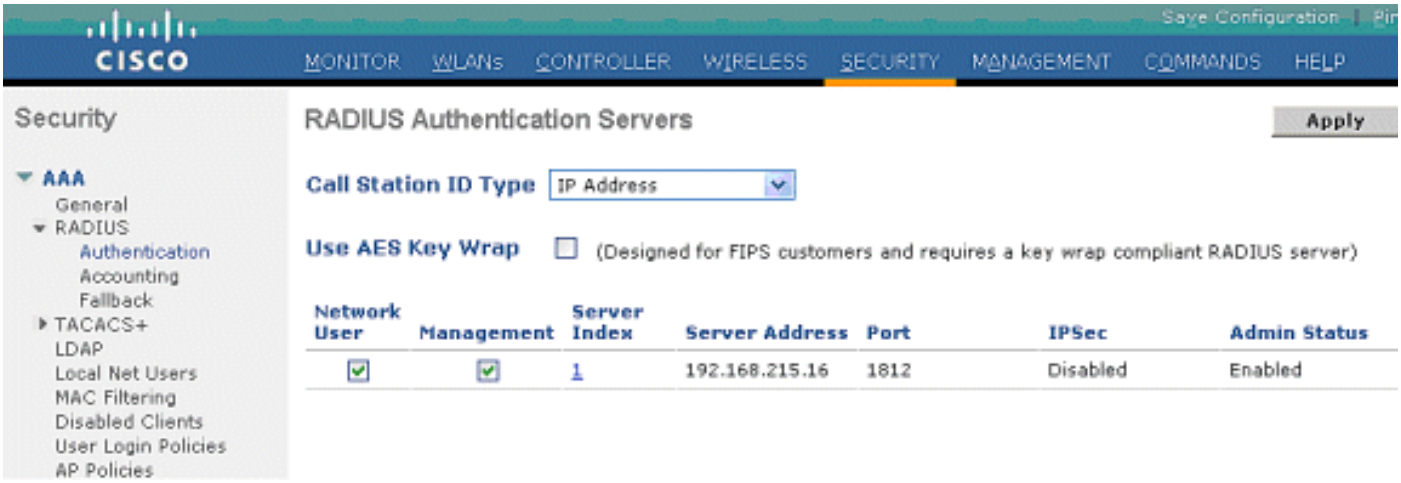
Configuration de NTP sur WLC



Un serveur de comptabilité de RAYON est prié de sorte que le serveur NGS puisse tracer l'adresse IP source reçue dans les messages de Syslog ASA à l'invité qui utilise cette adresse à ce moment particulier.

Ces deux écrans affichent la configuration de l'authentification de RAYON et de la comptabilité de RAYON sur le contrôleur d'ancre WLC. La configuration RADIUS n'est pas exigée sur le contrôleur étranger.

Authentification RADIUS



Gestion des comptes RADIUS

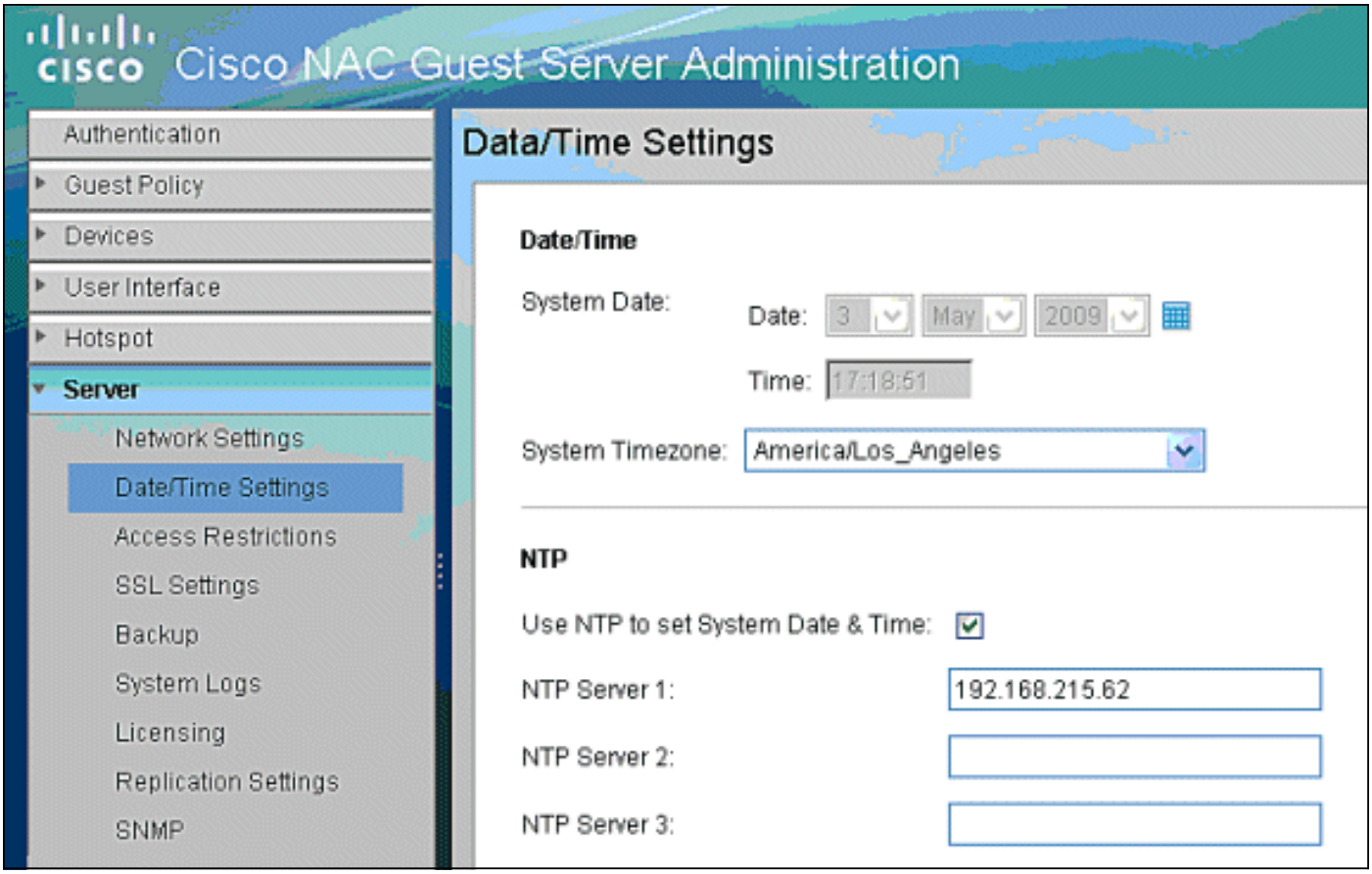
Configuration NGS

- NTP
- Clients RADIUS
- Syslog

Le serveur NGS est configuré de la page Web de https://(ip_address)/admin. Le nom d'utilisateur/mot de passe par défaut est admin/admin.

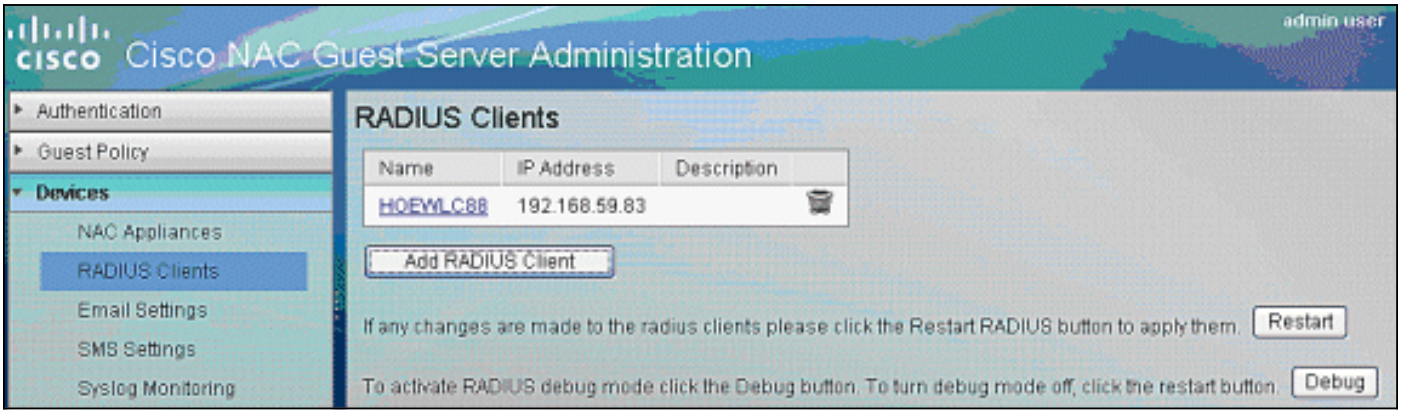
Des serveurs de NTP sont ajoutés dans l'écran de serveur/Date-Temps-configurations. L'il est recommandé que le fuseau horaire de système soit placé au fuseau horaire où le serveur est physiquement localisé. Quand le NTP est synchronisé, vous voyez un message au bas de cet écran qui indique, « état : Serveurs actifs de NTP » avec l'adresse IP qui affiche « la source temporelle en cours. »

Configuration de NTP NGS



Le serveur NGS doit être configuré avec l'adresse IP du contrôleur d'ancre en tant que client RADIUS. Cet écran se trouve à la page Devices/RADIUS-Clients. Assurez-vous que le secret partagé est identique qu'a été entré sur le contrôleur d'ancre. Cliquez sur le bouton de **reprise** après que vous apportiez des modifications pour redémarrer le service RADIUS sur le serveur NGS.

Clients RADIUS



Par défaut, le serveur NGS reçoit des messages de Syslog de n'importe quelle adresse IP. En conséquence, il n'y a aucune étape supplémentaire exigée pour recevoir les messages de Syslog de l'ASA.

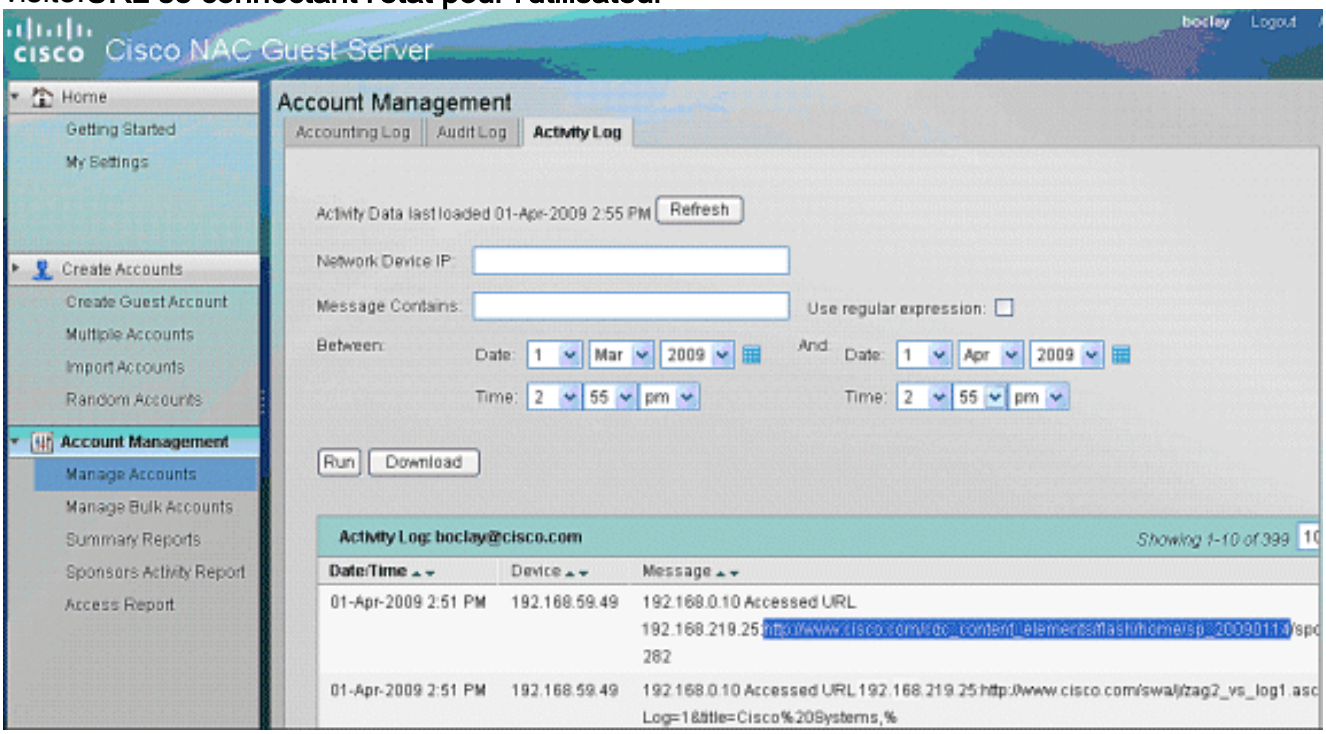
Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Suivez ces étapes pour vérifier qu'URL se connectant des travaux correctement.

1. D'un PC client, connectez au réseau Sans fil d'invité. Le PC reçoit une adresse IP, une passerelle par défaut, et un serveur DNS du serveur DHCP dans le contrôleur d'ancre.
2. Ouvrez un navigateur Web. Vous êtes réorienté à un écran de connexion. Écrivez un nom d'utilisateur et mot de passe d'invité. Sur l'authentification réussie, vous êtes réorienté à une page sur Internet par défaut.
3. Parcourez à de diverses pages Web sur l'Internet.
4. Connectez un PC de Gestion au NGS chez https:///(ip_address) et la procédure de connexion en tant que sponsor.
5. **Gestion des comptes de** clic. Vous voyez une liste de comptes d'invité. (Si votre compte d'invité n'apparaît pas, cliquez sur le bouton de **recherche avancée** et effacez le filtre qui spécifie que ce sponsor peut seulement voir les comptes qu'ils ont créés.)
6. Trouvez le compte utilisateur d'invité de la liste. Faites défiler vers la droite jusqu'à ce que vous voyiez l'icône de détails. Cliquez sur l'icône de **détails**.
7. Cliquez sur l'onglet de **journal d'activité**. Vous voyez une liste de l'URLs que l'invité a visité.**URL se connectant l'état pour l'utilisateur**



L'état prouve que l'utilisateur d'invité a visité http://www.cisco.com le 1er avril 2009 à 2:51 P.M. L'adresse de périphérique de 192.168.59.49 est l'adresse IP de l'ASA qui a envoyé le message de Syslog contenant le log URL. L'adresse IP source pour les utilisateurs d'invité est 192.168.0.10. L'adresse de destination est 192.168.219.25 pour http://www.cisco.com.

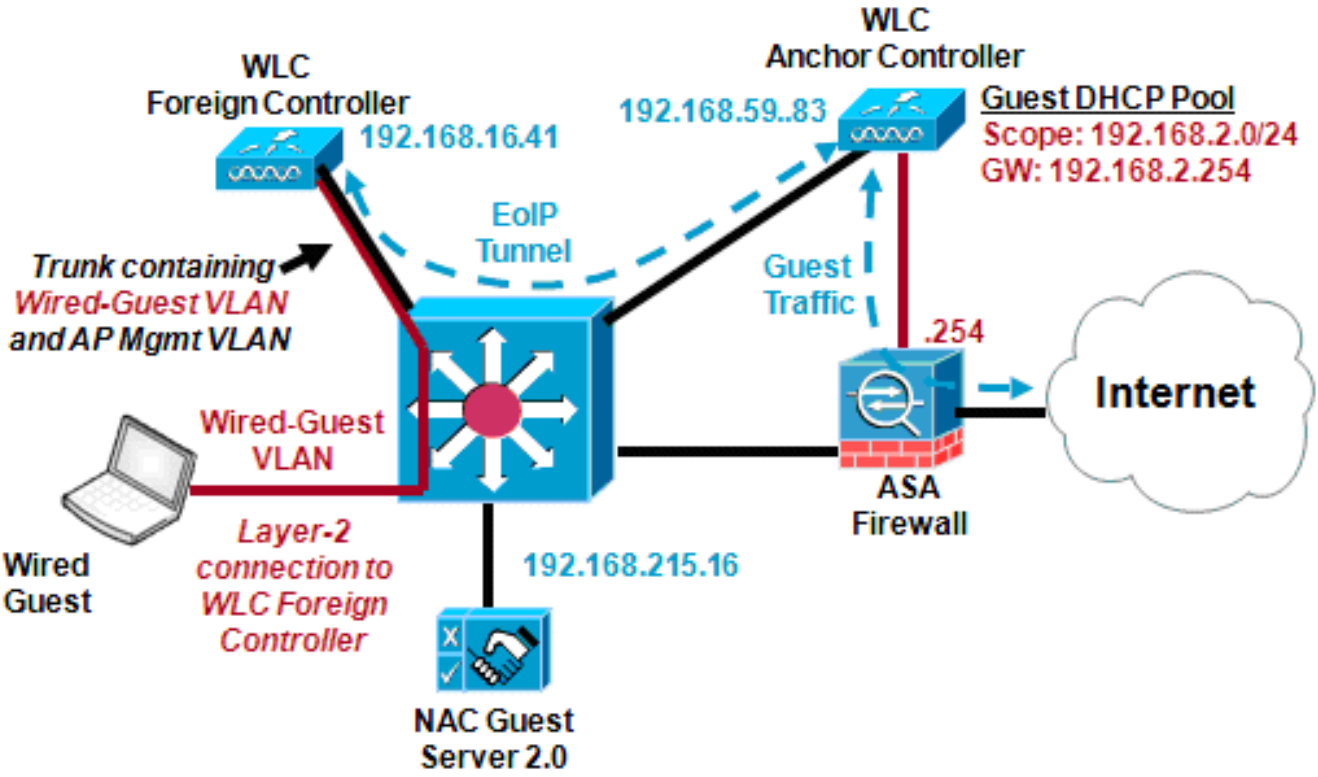
Annexes

Annexe A – Option de Câbler-invité

Jusqu'à ce point, cet article a couvert « URL intégré se connectant et signalant du trafic d'invité » pour l'usage dans un réseau de « radio-invité ». Cette section fournit des détails pour configurer un « câbler-invité, » aussi bien. des Câbler-invités et les radio-invités peuvent être activés sur le même contrôleur étranger WLC.

C'est le schéma de réseau pour le laboratoire de réseau de Câbler-invité.

Topologie de travaux pratiques de Câbler-invité



La topologie de travaux pratiques de câbler-invité est semblable à la topologie de travaux pratiques de radio-invité, affichée plus tôt, excepté l'ajout d'un câbler-invité VLAN. Le câbler-invité VLAN, affiché en rouge, est une connexion Layer-2 entre le PC de câbler-invité et le contrôleur étranger WLC. Le trafic du câbler-invité est reçu par le contrôleur étranger WLC et envoyé par EoIP au contrôleur d'ancre WLC. Le contrôleur d'ancre WLC fournit le DHCP et les services d'authentification pour l'utilisateur de câbler-invité de la même manière qu'ils ont fourni ces services pour l'utilisateur de radio-invité. La passerelle par défaut est l'ASA, et le serveur DNS est un serveur public sur l'Internet. Logiquement, tout le trafic dans et hors du sous-réseau est protégé par l'ASA.

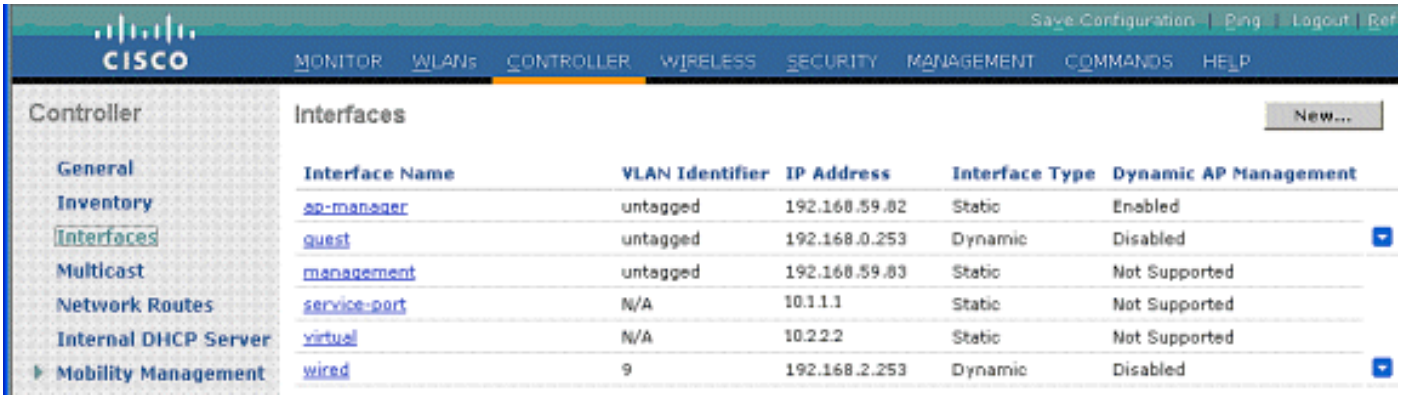
Il est recommandé pour ne pas configurer une interface Layer-3 sur le Câbler-invité VLAN puisque ceci peut permettre à un point de saut-hors fonction pour que le trafic coule hors du câbler-invité VLAN dans le réseau d'entreprise.

Annexe B – Configurations détaillées pour le WLCs

Contrôleur d'ancre WLC

Interfaces de contrôleur d'ancre

La configuration des interfaces sur le contrôleur d'ancre est affichée :



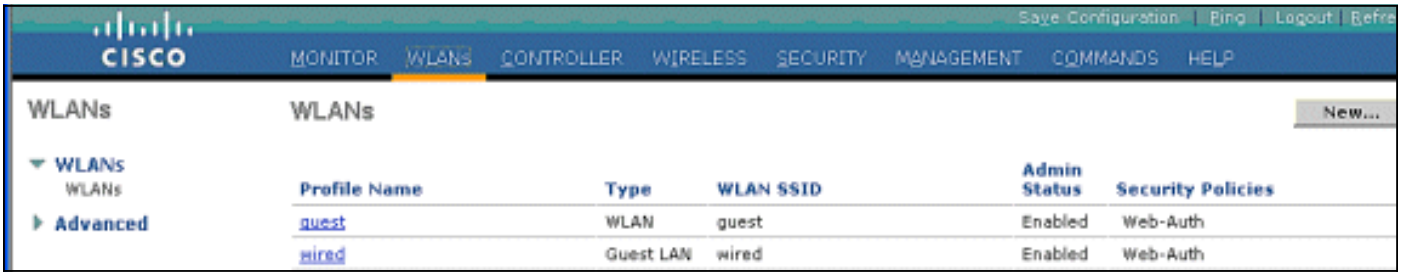
L'AP-gestionnaire et les interfaces de gestion sont sur le VLAN indigène du port physique 1 du WLC. Le port 1 se connecte au commutateur de Catalyst et reçoit le trafic du réseau client. Le trafic d'invité est reçu par le tunnel d'EoIP du contrôleur étranger et se termine par ce port.

L'interface d'invité est sur le VLAN indigène du port 2, et l'interface de câble est sur VLAN 9 du port 2 du port 2. se connecte à l'ASA et est utilisée pour envoyer le trafic à l'Internet.

Groupes de mobilité de contrôleur d'ancre

Pour cet exemple, un groupe de mobilité est configuré pour le contrôleur étranger (de câble) et un groupe de mobilité distinct pour le contrôleur d'ancre (ancre). La configuration sur le contrôleur d'ancre est affichée.

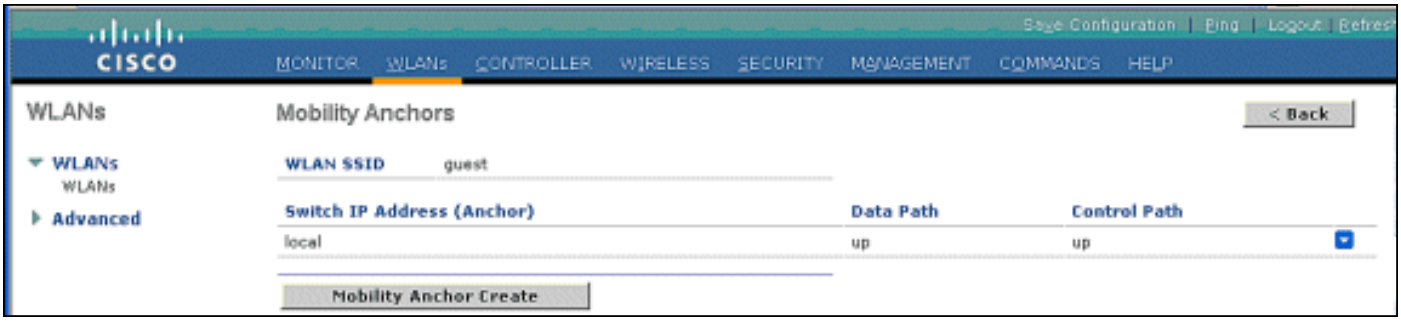
Contrôleur WLAN d'ancre



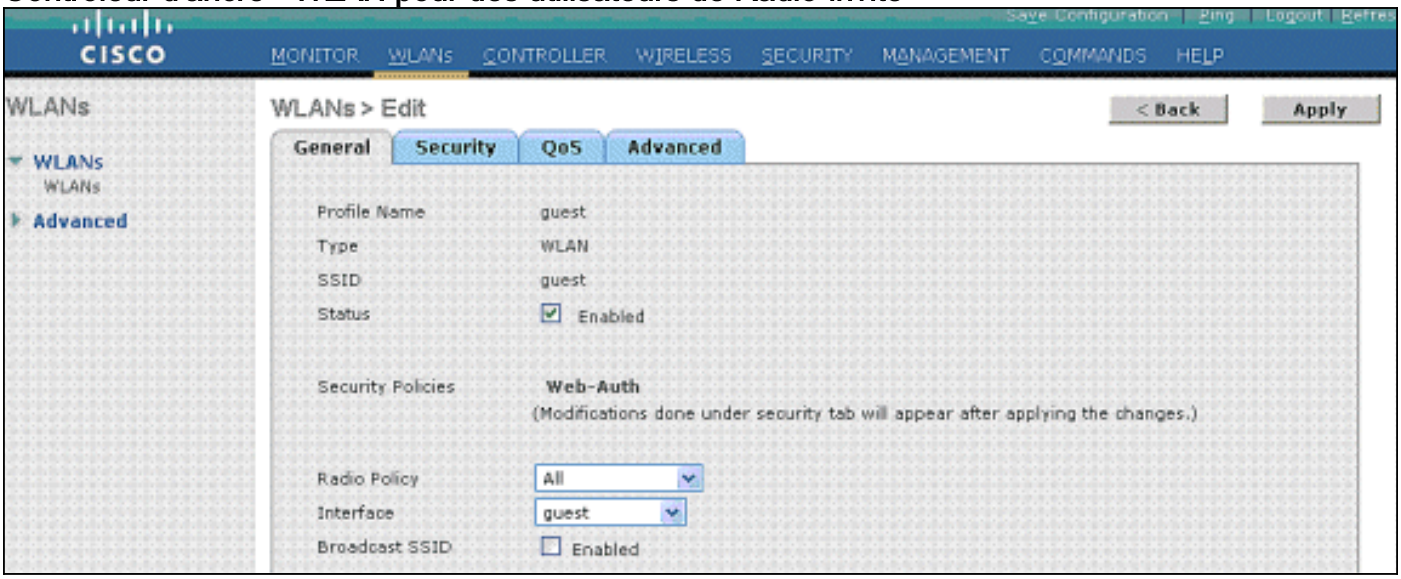
Contrôleur d'ancre - Placez l'ancre pour l'invité WLAN

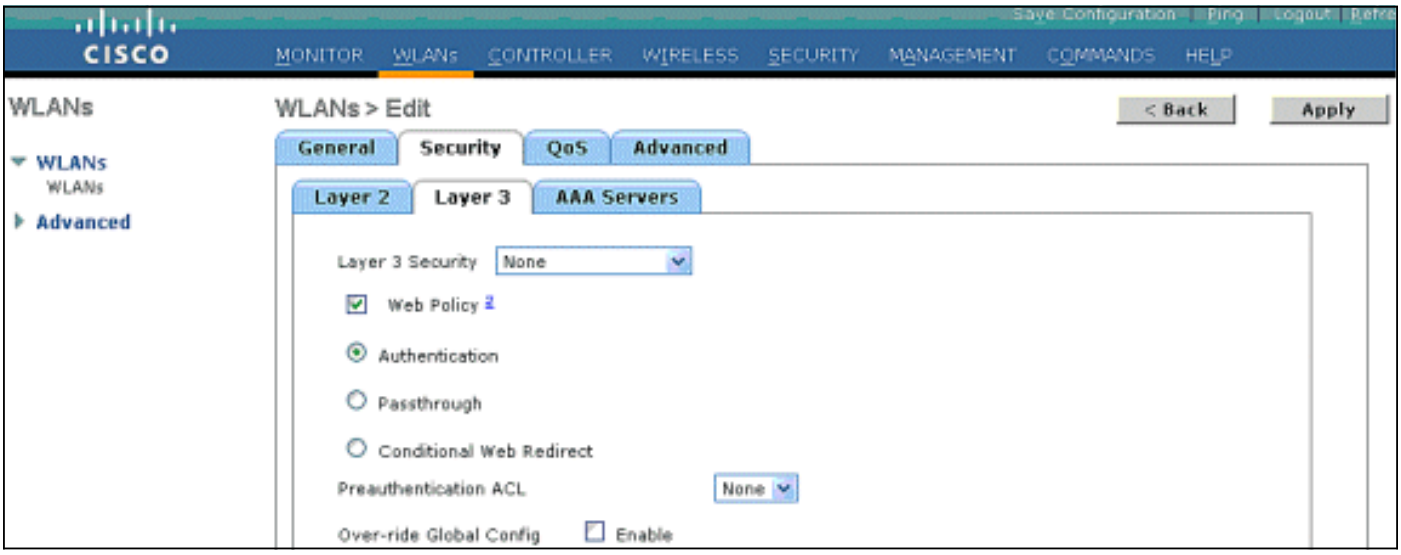
Afin de configurer ou les shows mobility anchors pour un WLAN, déplacent votre souris à la flèche déroulante à la droite, et choisissent des **ancres de mobilité**, comme affiché.

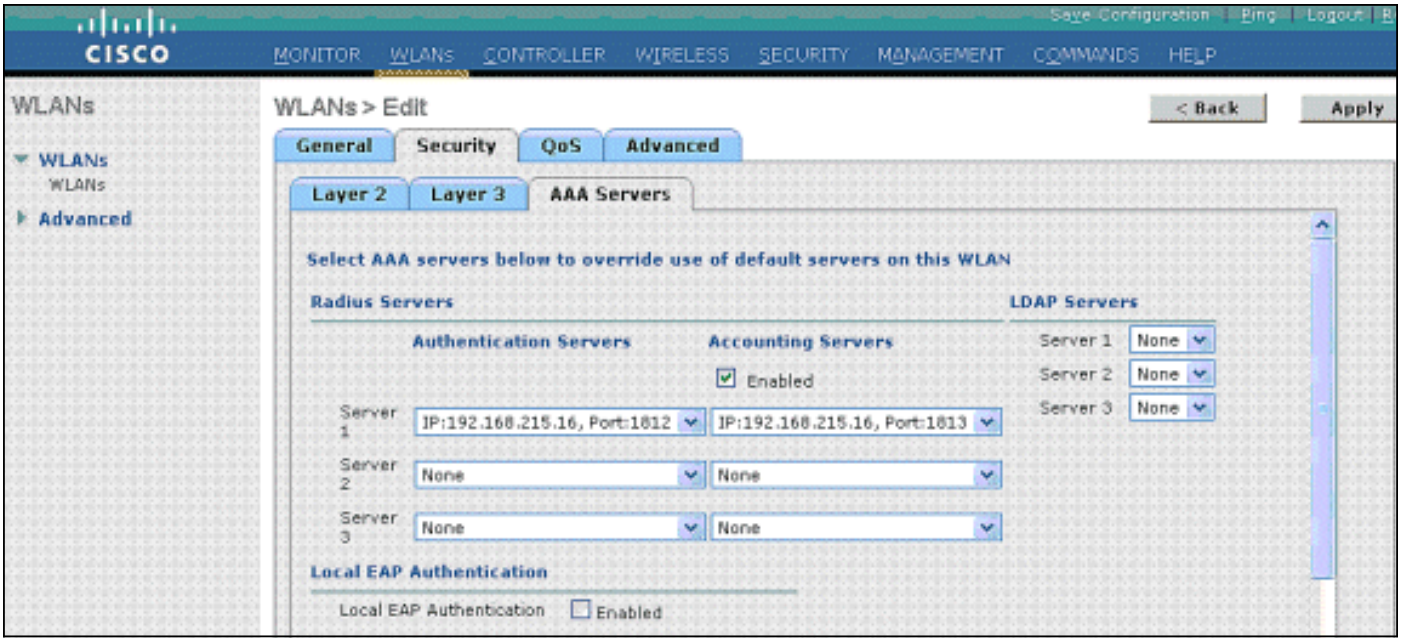
Contrôleur d'ancre - Placez l'ancre à lui-même

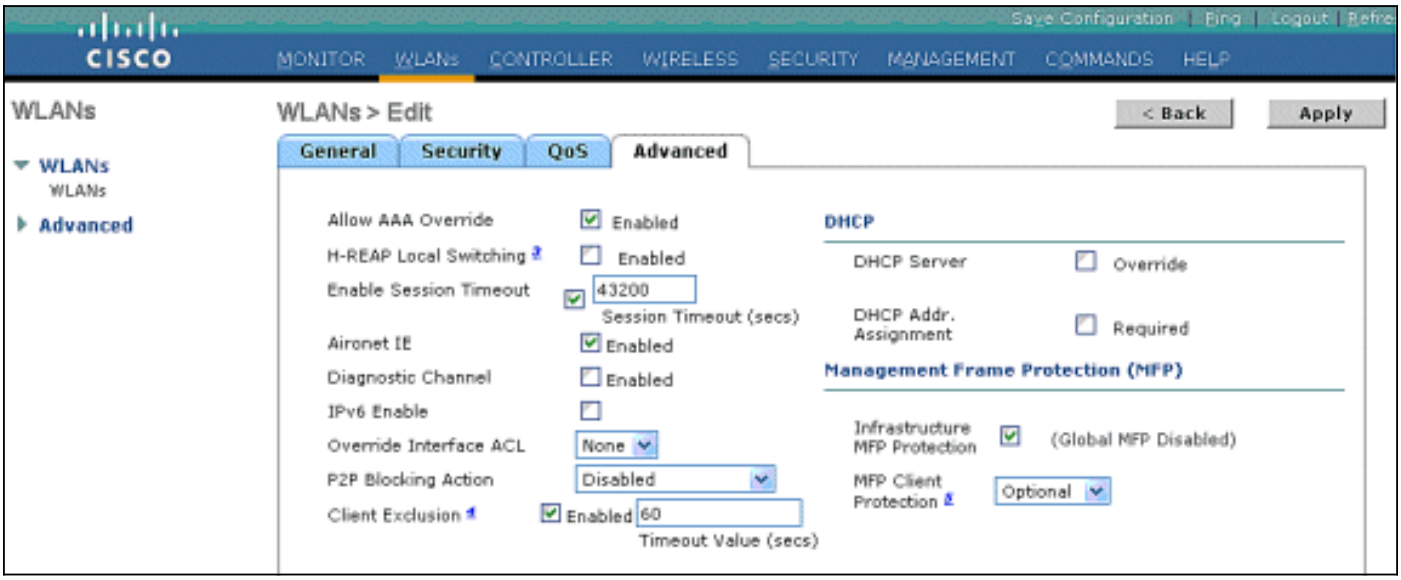


Contrôleur d'ancre - WLAN pour des utilisateurs de Radio-invité

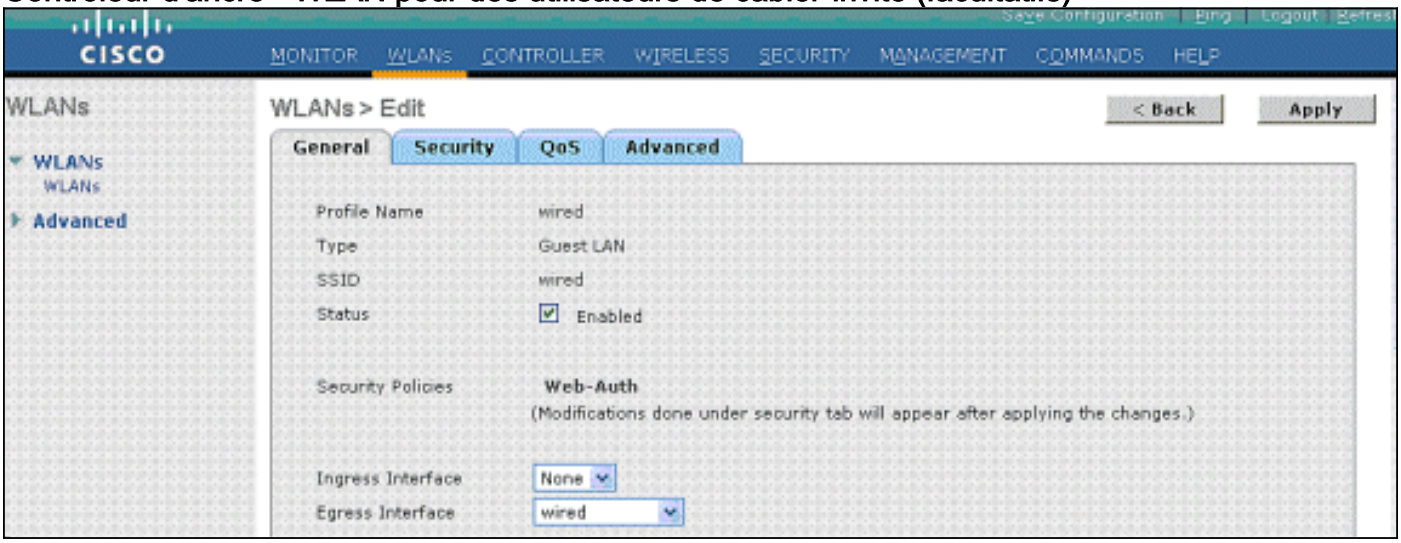


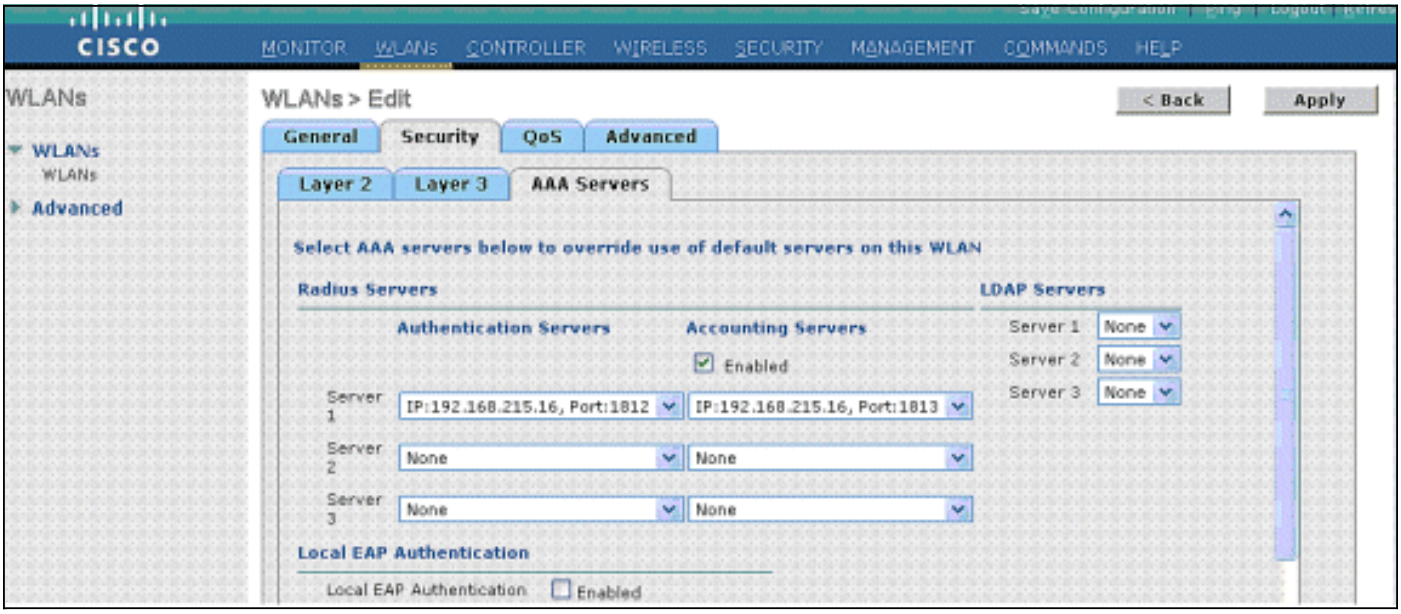


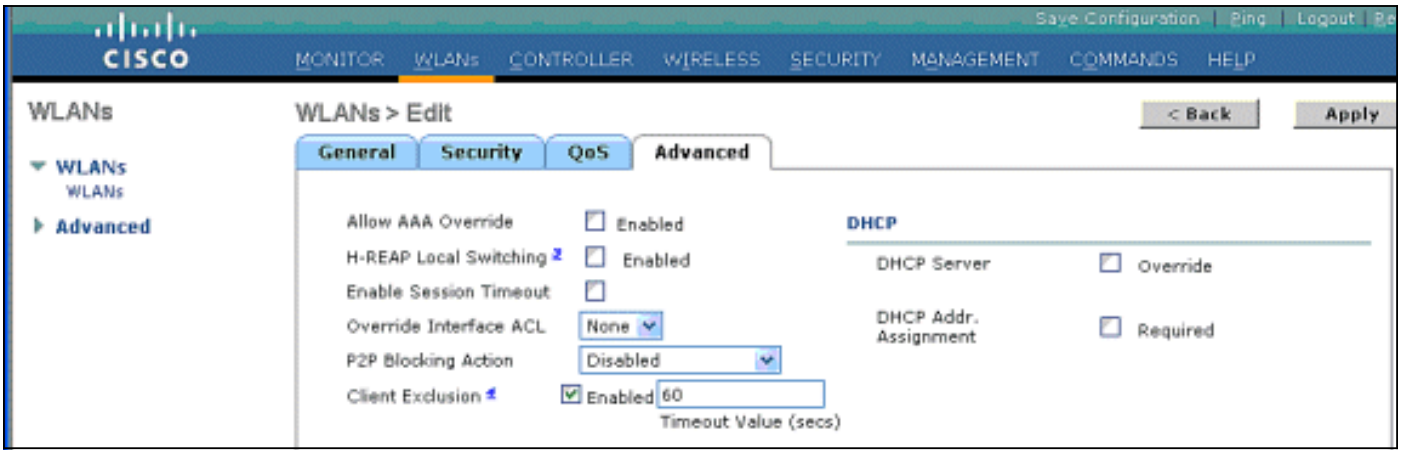




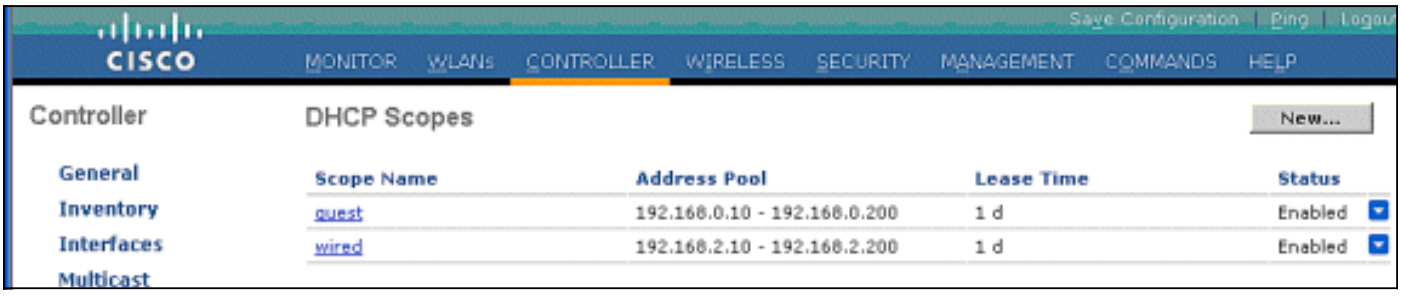
Contrôleur d'ancre - WLAN pour des utilisateurs de câbler-invité (facultatifs)



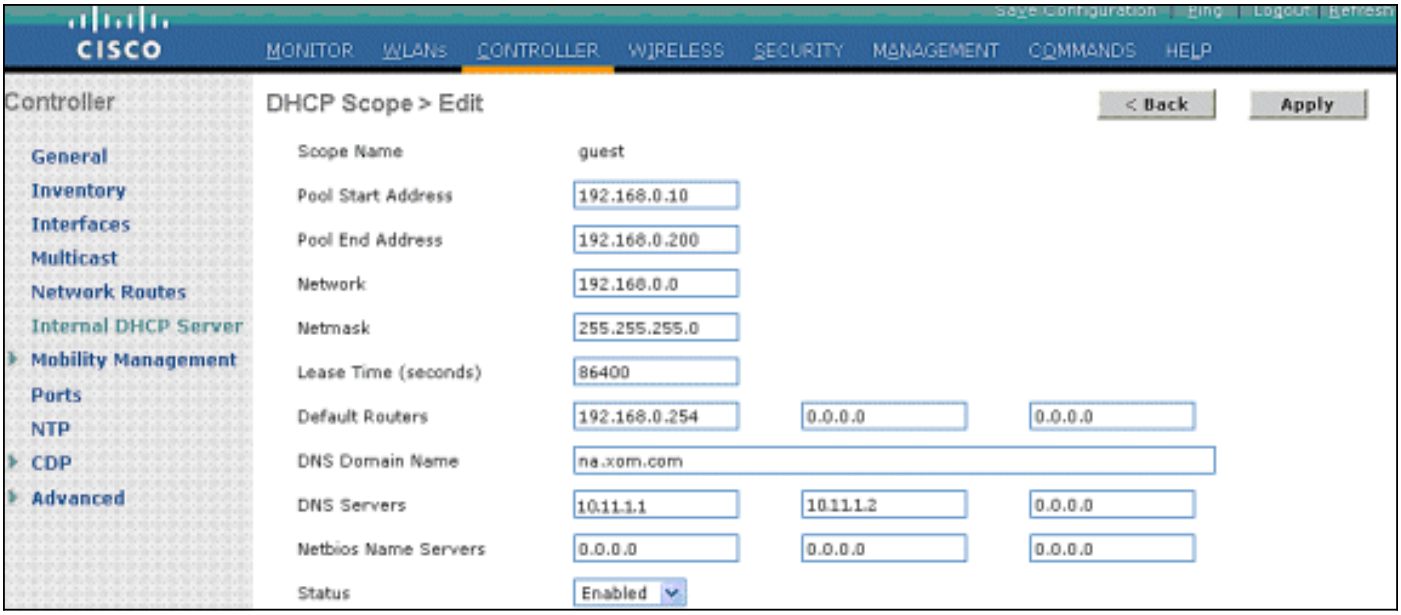




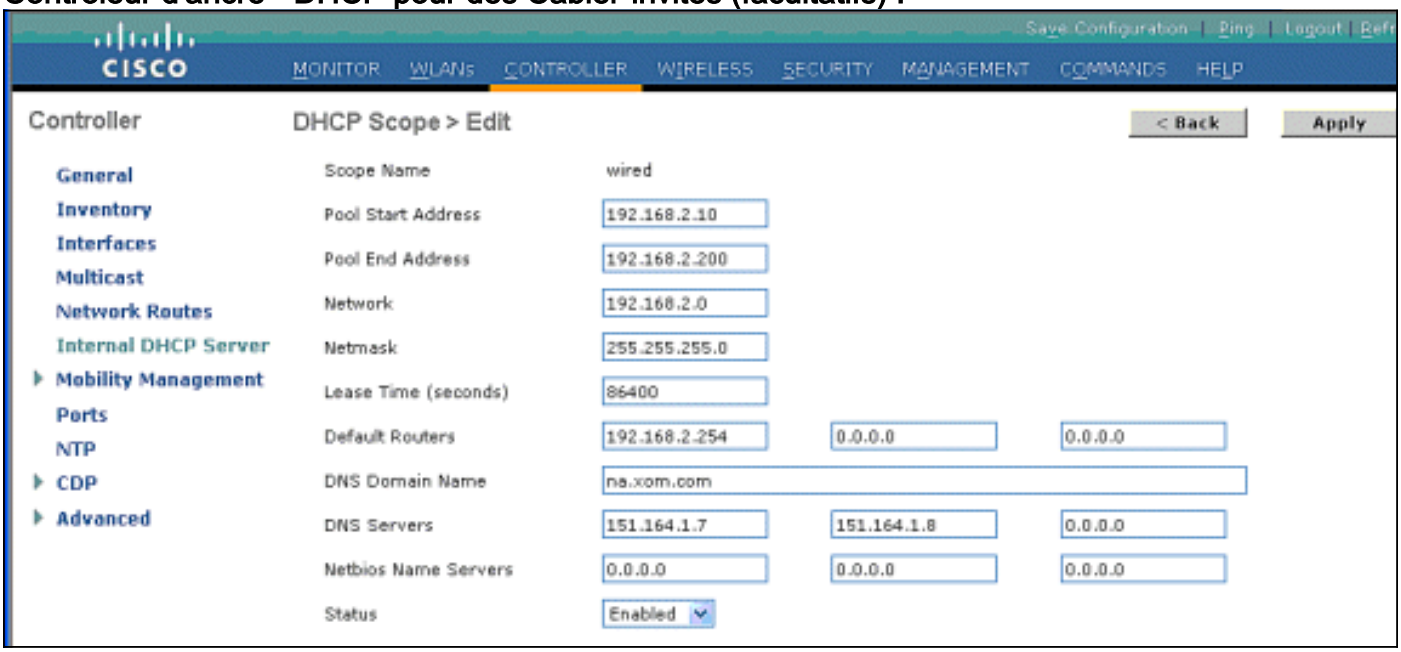
Contrôleur d'ancre - Portées de DHCP



Contrôleur d'ancre - Portée de DHCP pour des Radio-invités :



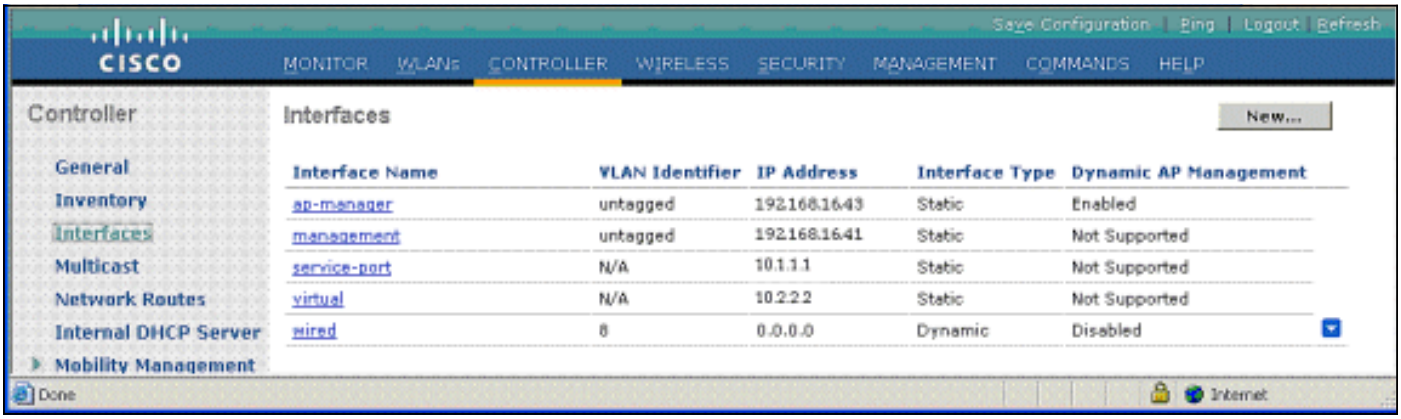
Contrôleur d'ancre - DHCP pour des Câbler-invités (facultatifs) :



Contrôleur étranger WLC

Interfaces

La configuration des interfaces sur le contrôleur étranger est affichée.

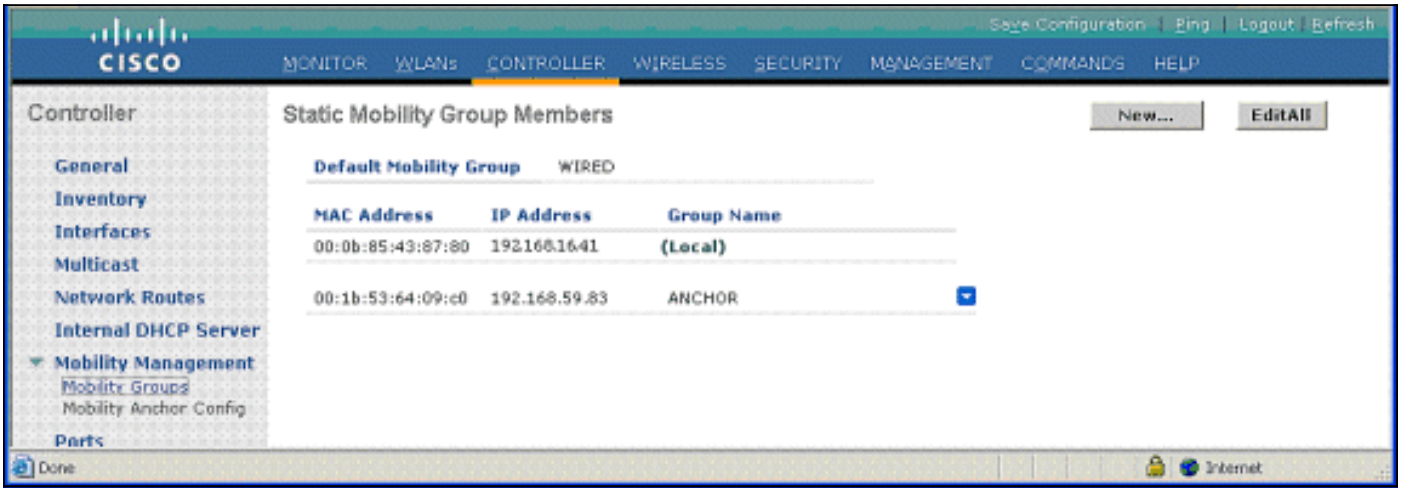


L'AP-gestionnaire et les interfaces de gestion sont sur le VLAN indigène du port physique 1 du WLC.

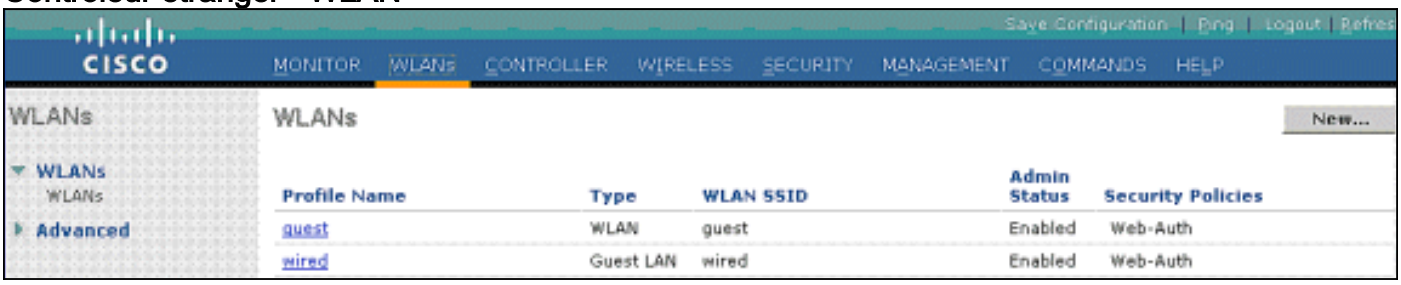
L'interface de câble est *facultative* et est seulement exigée si vous voulez fournir l'accès de câbler-invité. L'interface de câble est sur VLAN 8 du port physique 1. Cette interface reçoit le trafic de l'invité VLAN du commutateur de Catalyst et lui envoie le tunnel d'EoIP, par le VLAN indigène, au contrôleur d'ancre.

Contrôleur étranger - Groupes de mobilité

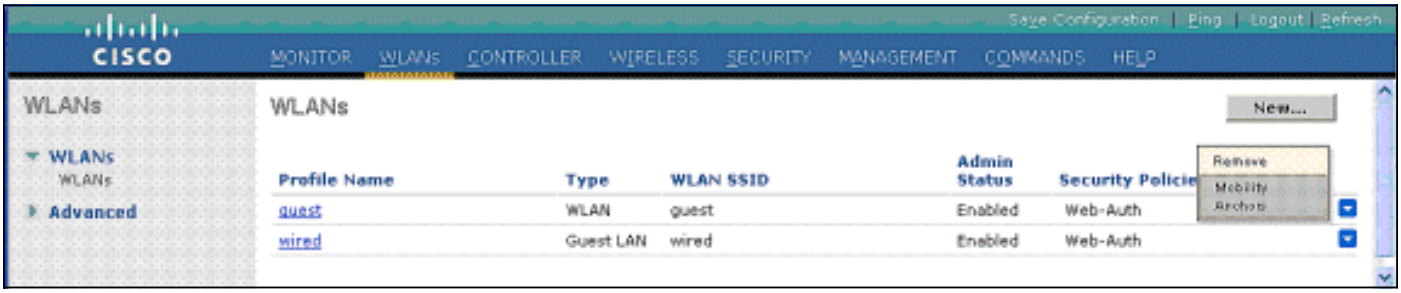
La configuration sur le contrôleur étranger est affichée.



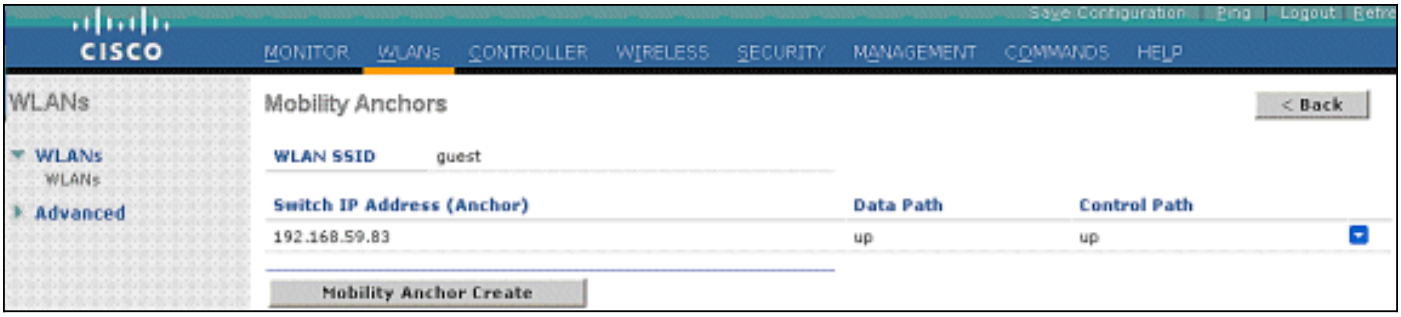
Contrôleur étranger - WLAN



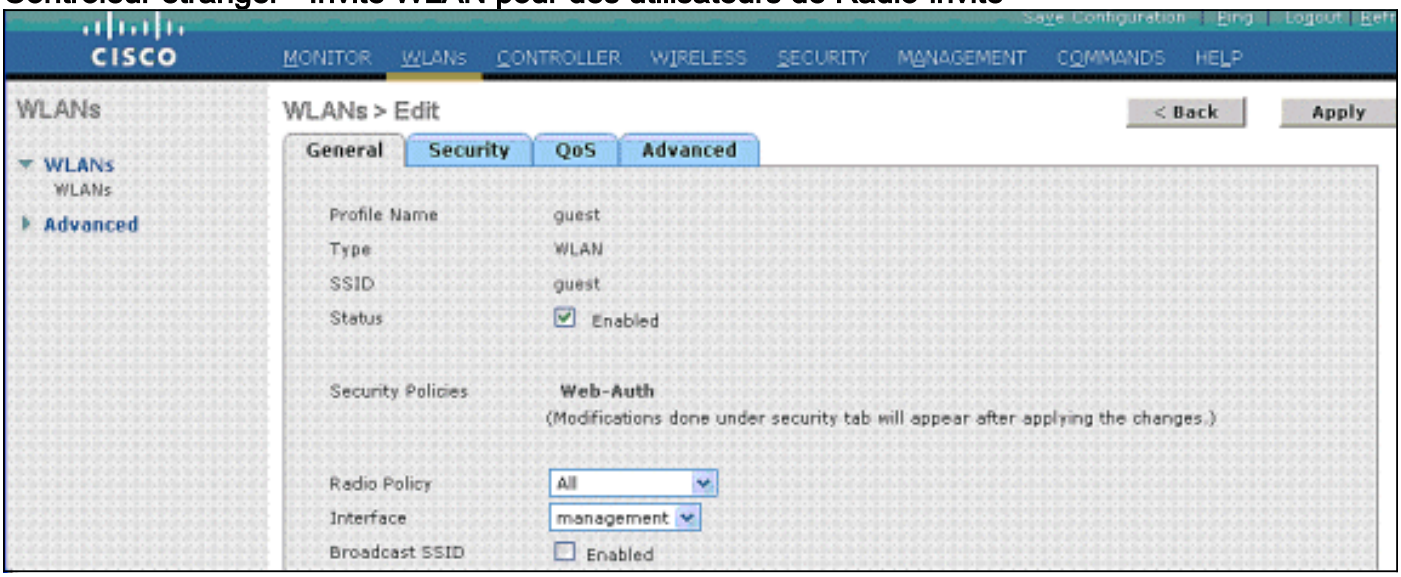
Afin de configurer ou les shows mobility anchors pour un WLAN, déplacent votre souris au-dessus de la flèche déroulante à la droite et choisissent des **ancres de mobilité**, comme affiché.

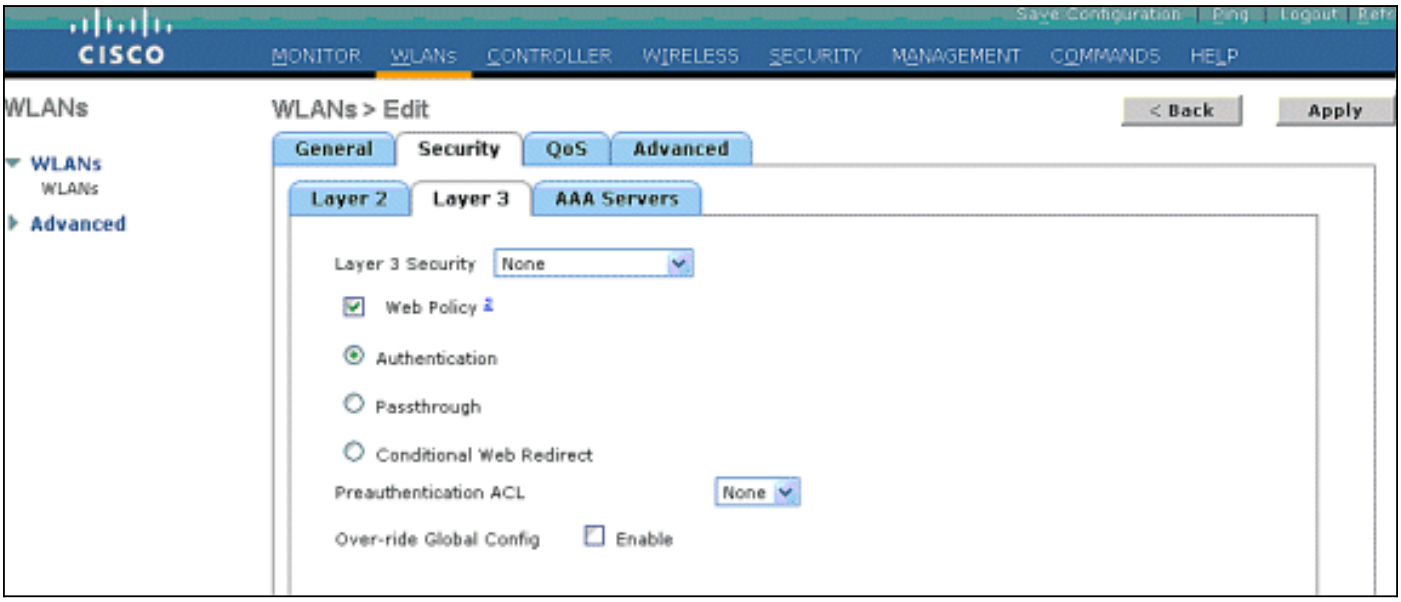


Positionnement d'ancre de mobilité pour ancrer le contrôleur

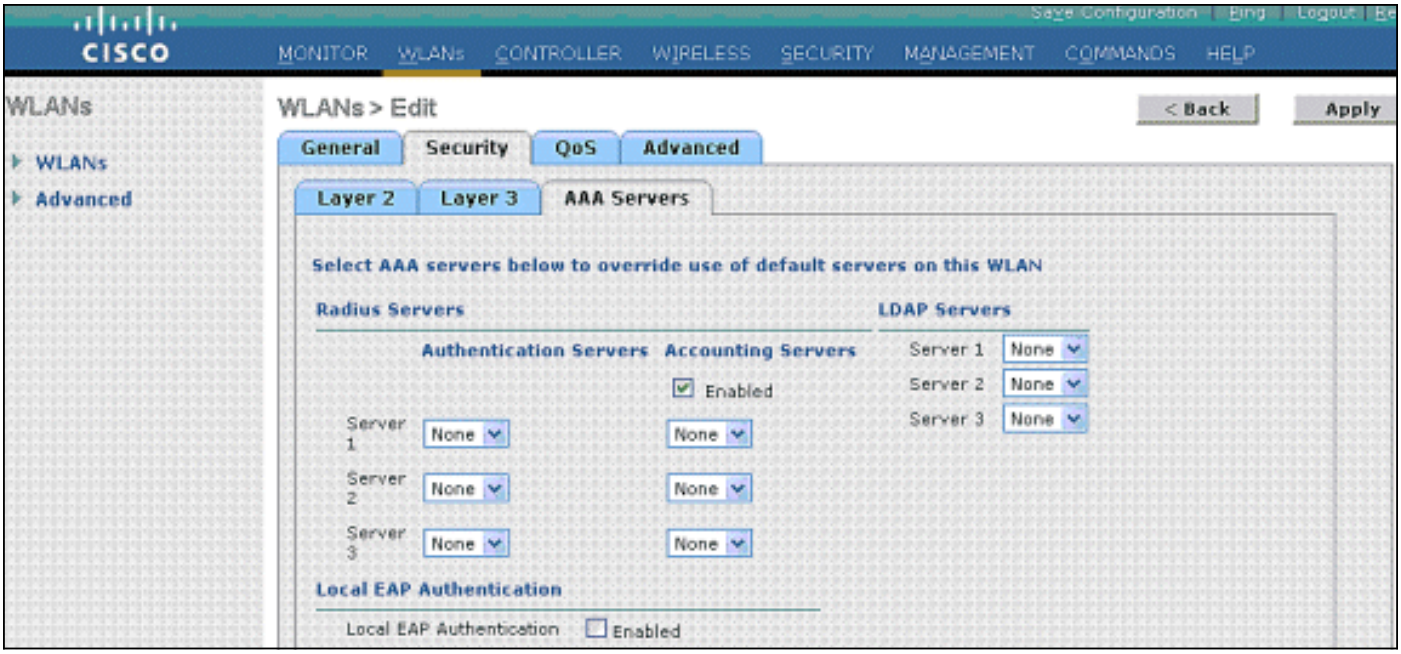


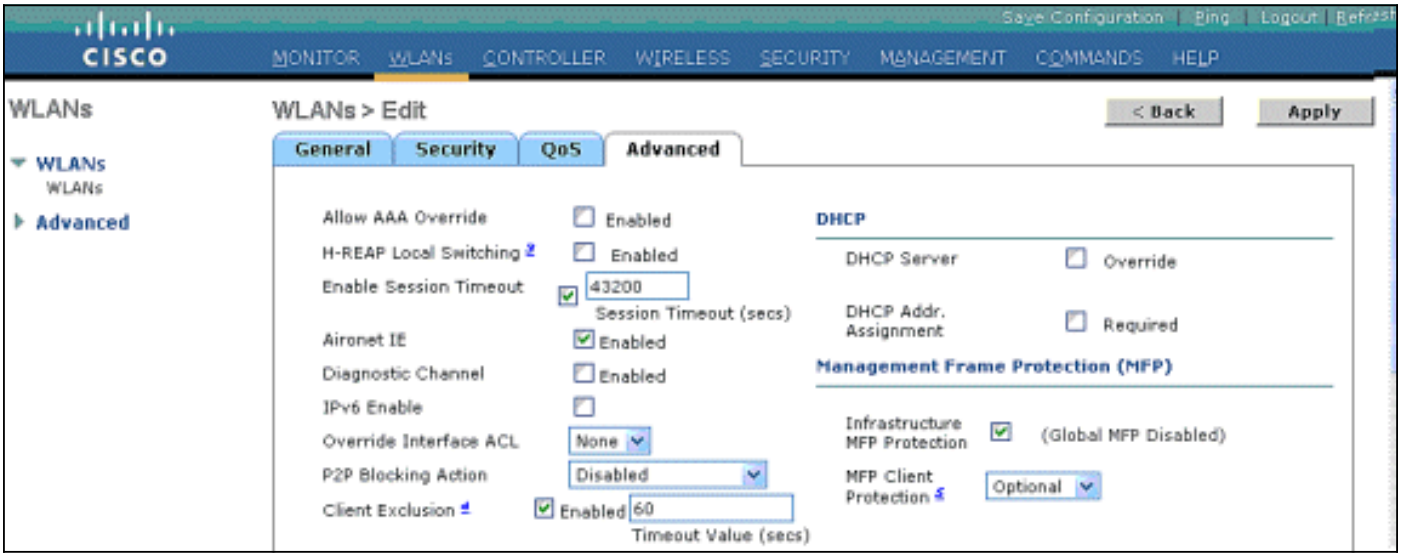
Contrôleur étranger - Invité WLAN pour des utilisateurs de Radio-invité



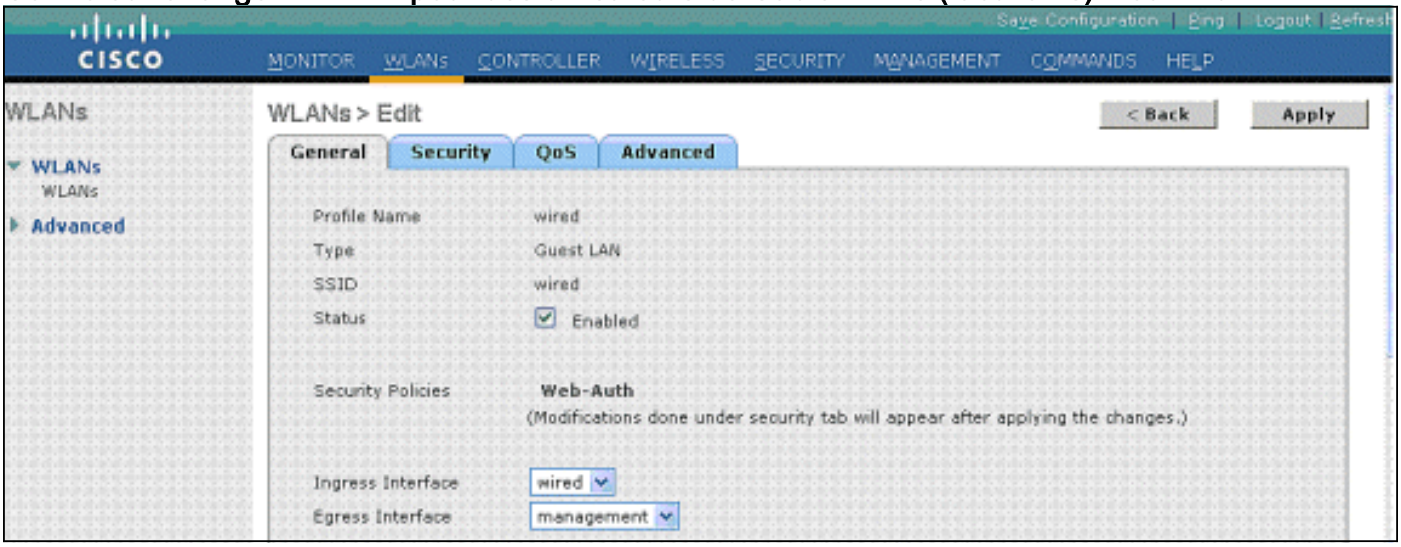


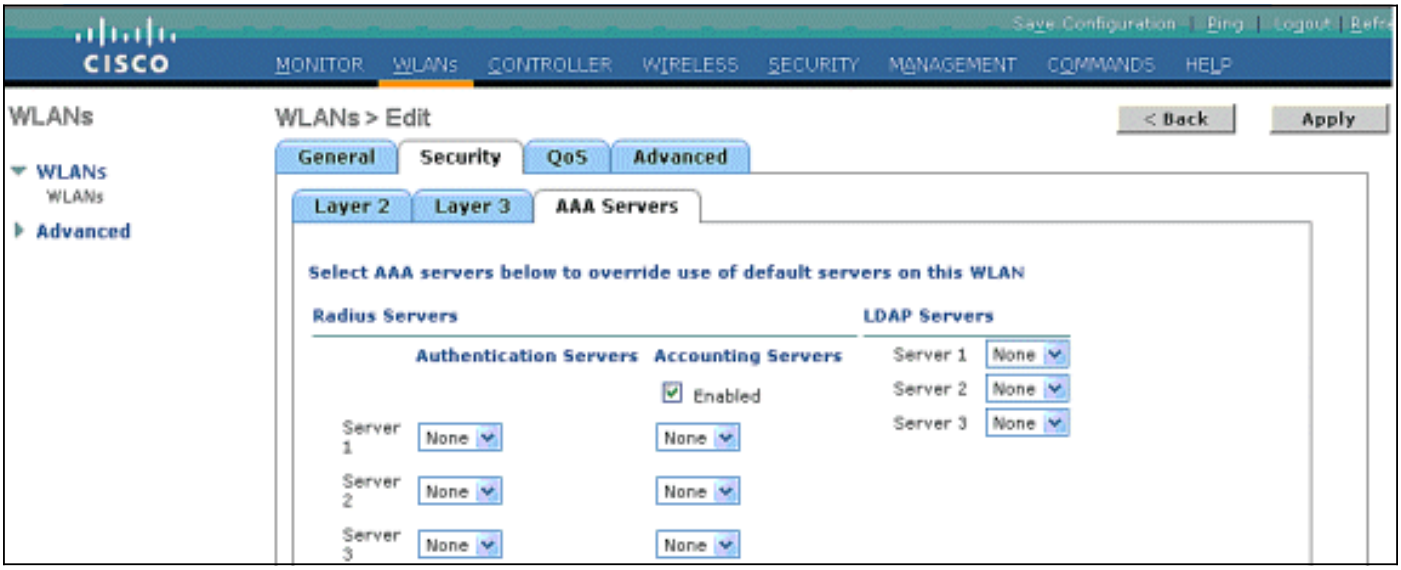
S

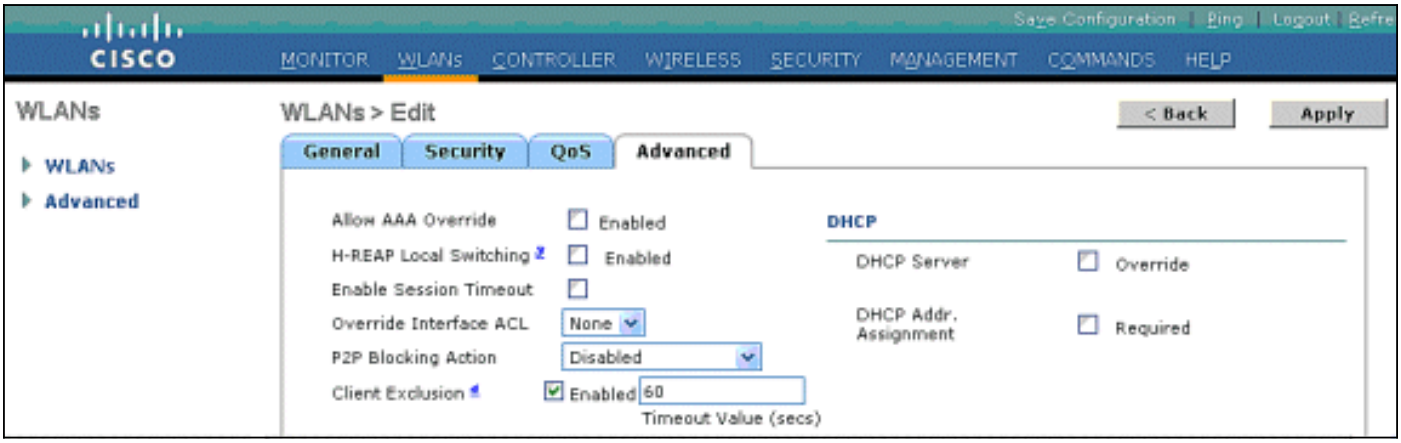




Contrôleur étranger - WLAN pour des utilisateurs de Câbler-invité (facultatifs) – continu







Annexe C – Configuration ASA

```
ASA-5520# show run
:
ASA Version 8.0(4)26
!
hostname ASA-5520
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.59.49 255.255.255.240
```

```
!
interface GigabitEthernet0/2
   <- Guest traffic enters this interface
 nameif wireless_guest
 security-level 50
 ip address 192.168.0.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.99.1 255.255.255.0
 management-only
!
boot system disk0:/asa804-26-k8.bin
clock timezone CST -6
clock summer-time CDT recurring
logging enable
logging timestamp
   <- provide a timestamp in each syslog message
logging list WebLogging message 304001
   <- list includes URL Log message (304001)
logging console errors
logging buffered notifications
logging trap WebLogging
   <- Send this list of Log messages to syslog servers
logging asdm informational
logging facility 21
logging host inside 192.168.215.16
   <- NGS is the syslog server
asdm image disk0:/asdm-61551.bin
route inside 10.10.10.0 255.255.255.0 192.168.59.62 1
route inside 192.168.215.0 255.255.255.0 192.168.59.62 1
route inside 198.168.1.15 255.255.255.255 192.168.59.62 1
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.99.0 255.255.255.0 management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 198.168.1.15 <- Configure ntp server
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

```
  inspect http
   <- Enable http inspection on the global policy
!
service-policy global_policy global
   <- Apply the policy
prompt hostname context
Cryptochecksum:b43ff809eacf50f0c9ef0ae2a9abbc1d
: end
```

Informations connexes

- Service RADIUS (Remote Authentication Dial-In User Service)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems