

Exemple de configuration de proxy d'authentification Web

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Configurez le WLC](#)

[Configurez le fichier PAC](#)

[Créez l'ACL de Préauthentification](#)

[Dépannage rapide : Configurez le navigateur Web](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification Web afin de fonctionner avec une installation de proxy.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base Sans fil de contrôleur LAN
- Sécurité d'authentification Web

[Composants utilisés](#)

Les informations dans ce document sont basées sur un contrôleur LAN Sans fil de Cisco, version 7.0 et ultérieures.

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](#).

Configurez

Administrateurs réseau qui font envoyer à un serveur proxy sur leur réseau le trafic web d'abord au serveur proxy, qui transmet par relais alors le trafic à l'Internet. Les connexions entre le client et le serveur proxy peuvent utiliser un port TCP autre que le port 80 pour la transmission. Ce port est habituellement le port TCP 3128 ou 8080. Par défaut, l'authentification Web écoute seulement sur le port 80. Ainsi, quand un HTTP OBTIENNENT des feuilles l'ordinateur, il est envoyé au port de proxy mais est relâché par le contrôleur.

Cette section décrit comment configurer l'authentification Web afin de fonctionner avec un proxy installé :

1. Configurez le contrôleur LAN Sans fil de Cisco (WLC) afin d'écouter sur le port de proxy.
2. Configurez le fichier de la configuration automatique de proxy (PAC) afin de renvoyer l'adresse IP virtuelle directe.
3. Créez une liste de contrôle d'accès de Préauthentification (ACL) afin de permettre au client pour télécharger le fichier PAC avant l'authentification Web.

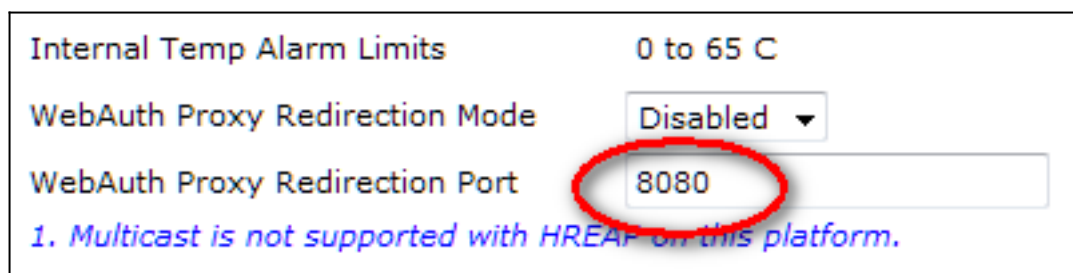
Comme dépannage rapide, vous pouvez configurer le navigateur Web manuellement afin de renvoyer 1.1.1.1.

Les détails sur chacun de ces processus sont dans les prochains paragraphes.

Configurez le WLC

Cette procédure décrit comment changer le port que le contrôleur écoute en fonction le port le serveur proxy écoute en fonction.

1. Naviguez vers le **contrôleur** > page **générale**.



The screenshot shows a configuration interface for a Cisco WLC. It features three rows of settings: 'Internal Temp Alarm Limits' with a value of '0 to 65 C', 'WebAuth Proxy Redirection Mode' with a dropdown menu set to 'Disabled', and 'WebAuth Proxy Redirection Port' with a text input field containing '8080'. The '8080' value is circled in red. Below the settings, there is a blue italicized note: '1. Multicast is not supported with HREF on this platform.'

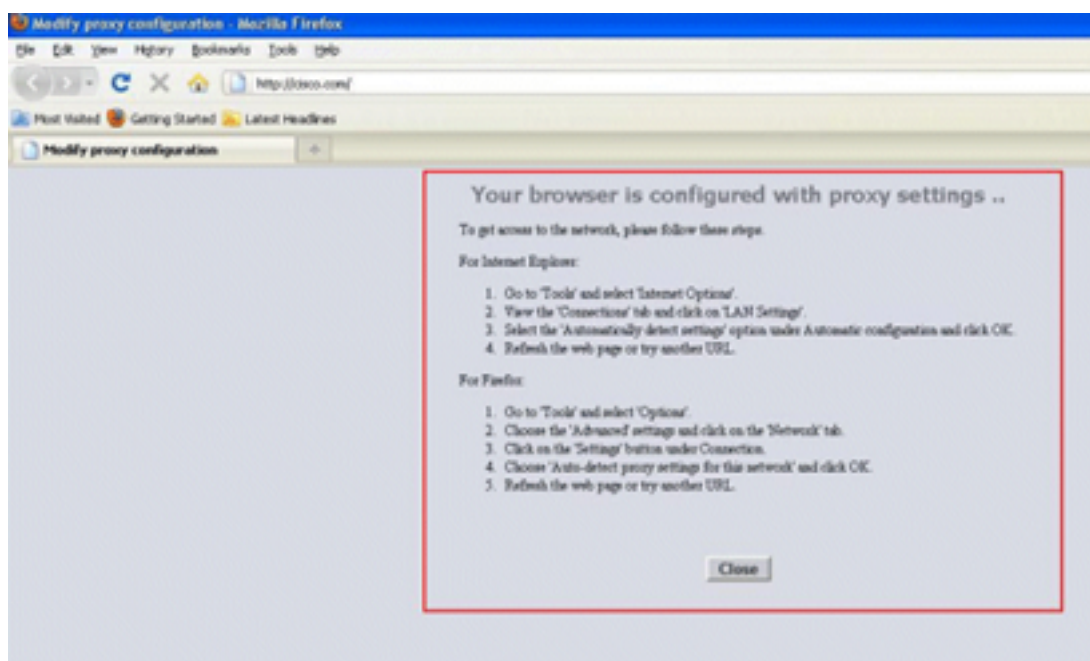
2. Dans le domaine de port de redirection de proxy de WebAuth, entrez dans le port que vous

voulez que le WLC écoute en fonction le client réorientez.

3. Handicapé choisi ou activé de la liste déroulante de mode de redirection de proxy de WebAuth :

Si vous sélectionnez **handicapé**, des clients sont présentés la page normale d'authentification Web pour la fonction émulation ou l'authentification. Ainsi, si vous utilisez un proxy, vous devez configurer tous les navigateurs de client pour ne pas utiliser le proxy pour 1.1.1.1 (ou toute autre adresse IP virtuelle les utilisations WLC). Voir le [dépannage rapide : Configurez le navigateur Web](#).

Si vous sélectionnez **activé**, le WLC écoute sur les ports 80, 8080, et 3128 par défaut, ainsi vous ne devez pas entrer dans ces ports dans le champ texte de port de redirection de proxy de WebAuth. Si un client envoie un HTTP OBTENEZ sur ces ports, ils voient un écran qui leur demande pour changer leurs paramètres de proxy à automatique.



4. Enregistrez la configuration.

5. Redémarrez le contrôleur.

En résumé, introduisez un numéro de port dans le port de redirection de proxy de WebAuth afin de définir le port que le WLC écoute en fonction. Quand le mode de redirection est activé, il réoriente le client à l'écran de paramètre de proxy et le compte pousser dynamiquement une détection automatique de proxy de Web (WPAD) ou le fichier PAC pour la configuration de proxy automatique. Une fois désactivé, le client est réorienté à la page normale d'authentification Web.

Configurez le fichier PAC

L'adresse IP virtuelle du WLC doit être « directe » retourné afin du Web authentique pour authentifier correctement des utilisateurs. Dirigez signifie que le serveur proxy ne fait pas proxy la demande, et le client a des autorisations d'atteindre directement à l'adresse IP. Ceci est habituellement configuré sur le serveur proxy dans le fichier WPAD ou PAC par l'administrateur de

serveur proxy. C'est un exemple de configuration pour un fichier PAC :

```
function FindProxyForURL(url, host) {  
    // our local URLs from the domains below example.com don't need a proxy:  
    if (shExpMatch(host, "*.example.com"))  
    if (shExpMatch(host, "1.1.1.1"))    <-- (Line states return 1.1.1 directly)    {  
        return "DIRECT";  
    }  
    // URLs within this network are accessed through  
    // port 8080 on fastproxy.example.com:  
    if (isInNet(host, "10.0.0.0", "255.255.248.0"))  
    {  
        return "PROXY fastproxy.example.com:8080";  
    }  
  
    // All other requests go through port 8080 of proxy.example.com.  
    // should that fail to respond, go directly to the WWW:  
    return "PROXY proxy.example.com:8080; DIRECT";  
}
```

Créez l'ACL de Préauthenticatifion

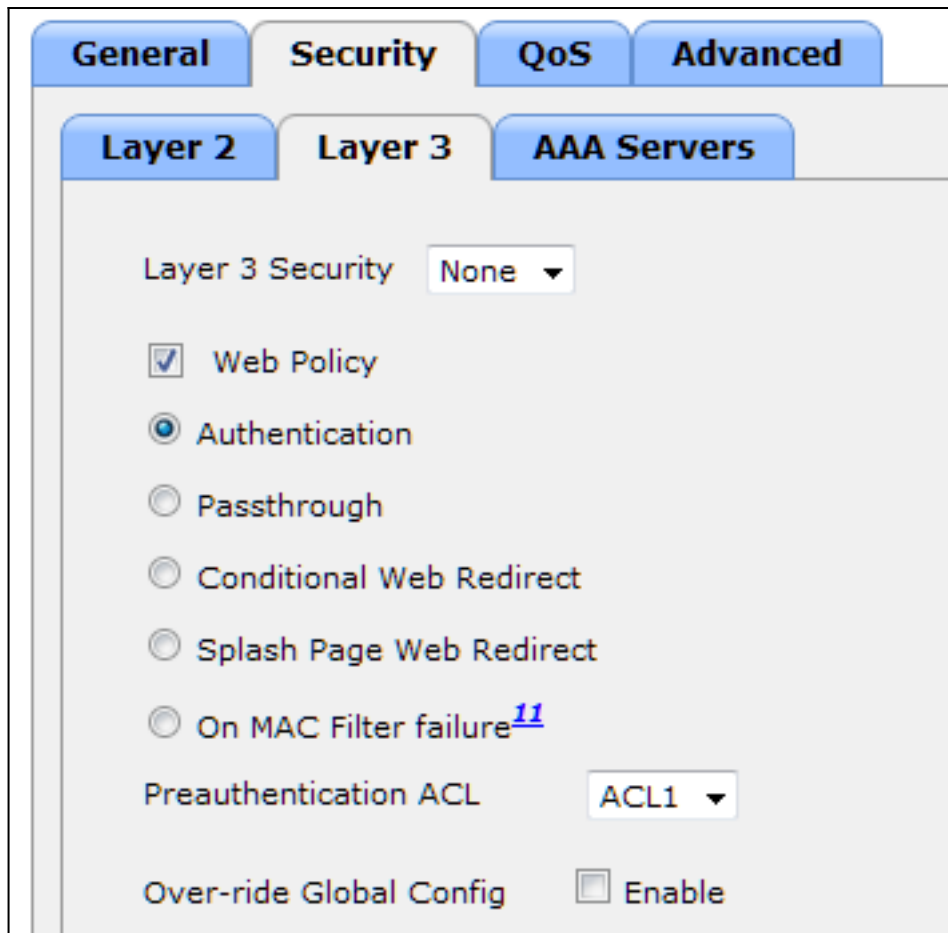
Placez un ACL de Préauthenticatifion sur l'Identifiant SSID (Service Set Identifier) d'authentification Web de sorte que les clients sans fil puissent télécharger le fichier PAC avant que les clients se connectent dans le Web authentique. Les besoins d'ACL de Préauthenticatifion de permettre à accès seulement au port le fichier PAC est allumés. Access au port de proxy permet à des clients pour atteindre l'Internet sans authentification Web.

1. Naviguez vers la **Sécurité** > la **liste de contrôle d'accès** afin de créer un ACL sur le contrôleur.
2. Créez les règles de permettre le trafic sur le port de téléchargement PAC au proxy dans les deux directions.

General										
Access List Name		ACL1								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	192.168.0.4 /	TCP	Any	8081	Any	Any	0	
		0.0.0.0	255.255.255.255							
2	Permit	192.168.0.4 /	0.0.0.0 /	TCP	8081	Any	Any	Any	0	
		255.255.255.255	0.0.0.0							

Remarque: Ne permettez pas le port HTTP de proxy.

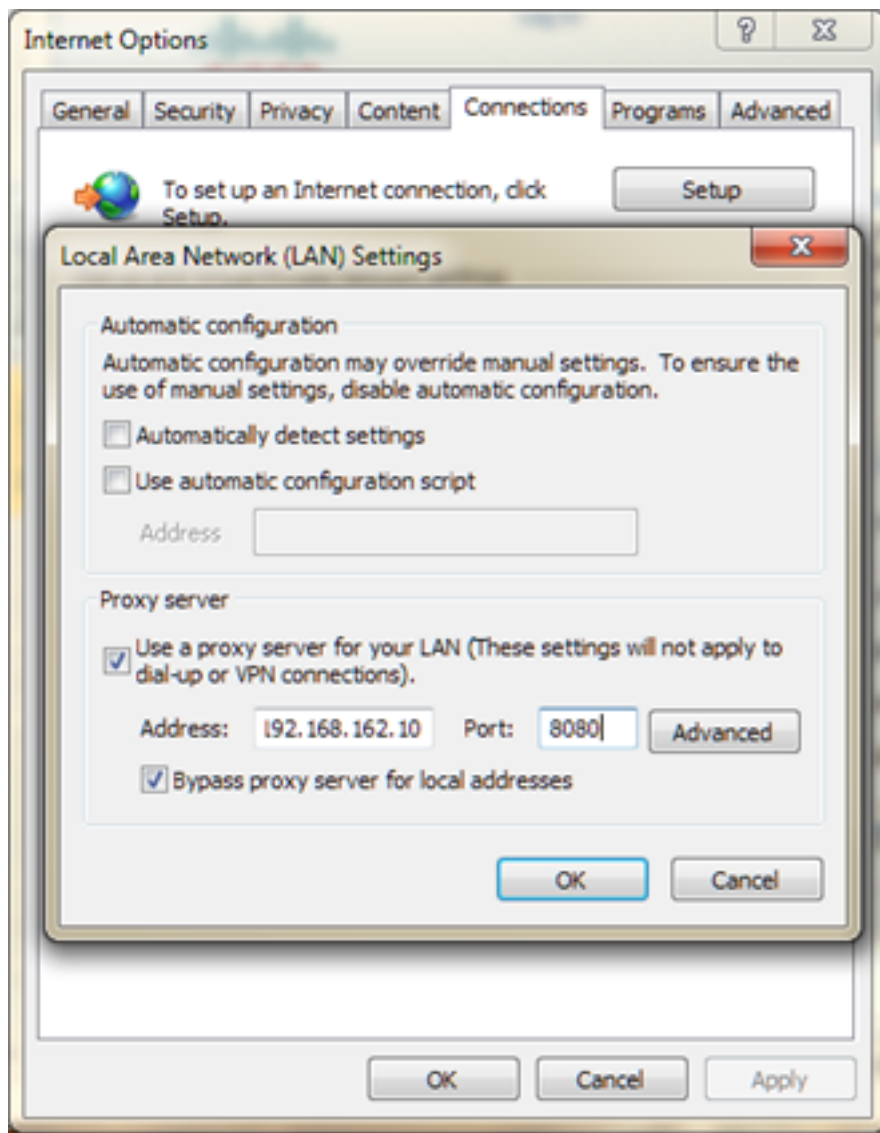
3. Dans la configuration WLAN sur le contrôleur, n'oubliez pas de sélectionner l'ACL que vous avez juste créé comme ACL de Préauthenticatifion.



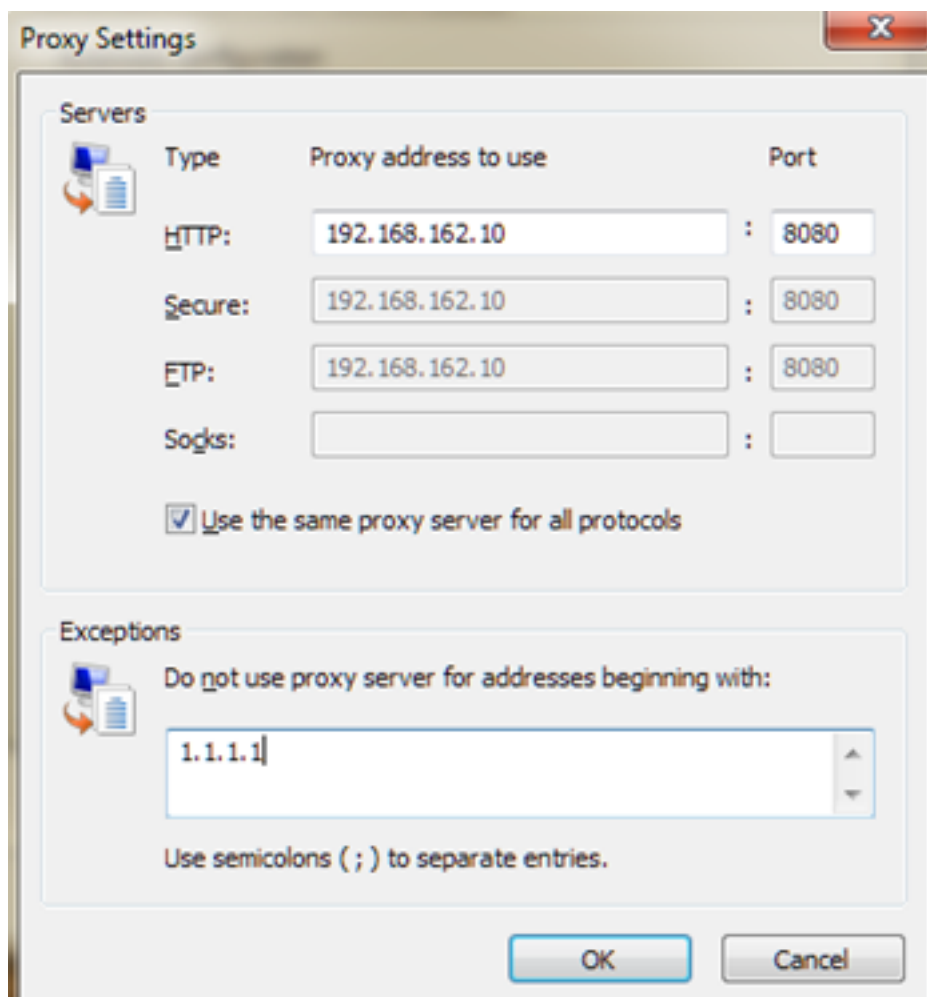
Dépannage rapide : Configurez le navigateur Web

Cette procédure décrit comment configurer manuellement une exception de sorte qu'un navigateur Web de client atteigne directement à 1.1.1.1.

1. En Internet Explorer, naviguez vers des **outils** > des **options Internet**.
2. Cliquez sur l'onglet de **connexions**, puis le **bouton Settings de RÉSEAU LOCAL**.
3. Dans la région de serveur proxy, l'**utilisation de** contrôle un **serveur proxy pour votre RÉSEAU LOCAL**, et introduisent l'adresse (IP) et mettent en communication le serveur écoute en fonction.



4. Cliquez sur le **bouton avancé** et écrivez l'adresse IP virtuelle du WLC dans la région d'exceptions.



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](#)

- [Support et documentation techniques - Cisco Systems](#)